THEORY of EQUATIONS

Cyrus Colton MacDuffee

PROFESSOR OF MATHEMATICS
UNIVERSITY OF WISCONSIN

JOHN WILEY & SONS, INC. NEW YORK
CHAPMAN & HALL, LTD. LONDON

Library of Congress Catalog Card Number: 54–5768

Printed in the United States of America

Preface

This small book is the outgrowth of a one-semester course given at the University of Wisconsin to classes of junior and senior students gathered from all colleges of the university. It is not easy to design a course that will at the same time please undergraduates in physics, chemistry, statistics, agriculture, engineering, and pure mathematics. This book is quite conservative in following the outlines of a standard course in the theory of equations but differs from it in the emphasis it places upon the theory of polynomials, a point of view that should be of particular value to students who expect to continue with mathematics. The small amount of abstract algebra that it contains should be painlessly absorbable even by those to whom it is not a primary interest. The computational aspect of the subject is not neglected. Determinants are not included in this book, for it has been our practice to postpone this topic to a second semester in order to have sufficient time for a really satisfactory course in matrices and determinants.

Acknowledgment is due to Dr. R. D. Wagner for a critical reading of the manuscript.

C. C. MacDuffee

The University of Wisconsin
November 1953

Contents

CHAPTER

1

Linear Systems

1. Solution of an Equation

The mathematical representation of a function, such as

$$f(x) = \frac{x^2 - 2x - 3}{4x + 1},$$

is like a builder's blueprint. It gives precise directions for obtaining a functional value $f(x_1)$ from a number x_1 on the range of definition of the function. Carrying out these directions is known as *substituting* the number x_1 for the variable x. Occasionally the directions are impossible to carry out, in which case the functional value does not exist. Thus in the above example $f(-\frac{1}{4})$ does not exist.

An equation such as

$$f(x) = \frac{x^2 - 2x - 3}{4x + 1} = 0$$

is the statement of a condition which an unknown number x must satisfy. A number x_1 which, when substituted for the unknown x, yields a functional value $f(x_1)$ equal to 0 is called a *solution* or *root* of the equation $f(x) = 0$. To *solve* an equation is to find all of its solutions. Clearly 3 and -1 are solutions of the above equation, and there are no others.

A method frequently employed in solving an equation is first to assume that the equation has a solution and then to find a set of numbers or "candidates" among which all solutions must lie. The ultimate test, however, comes upon substituting these "candidates" into the given equation, retaining only such as satisfy it.

Let us consider the equation

$$\sqrt{x^2 - 9} = \tfrac{4}{5}x$$

where, as always, the radical denotes the principal square root, i.e., the positive square root of the radicand when the latter is positive.

Let us assume that there is a number x_1 which satisfies the equation. Then, clearly,

$$\sqrt{x_1^2 - 9} = \tfrac{4}{5}x_1, \qquad x_1^2 - 9 = \tfrac{16}{25}x_1^2,$$

$$\tfrac{9}{25}x_1^2 - 9 = 0,$$

$$x_1^2 = 25, \qquad x_1 = \pm 5.$$

Thus there are only two candidates, and every solution of the equation is either 5 or -5. But we have not proved that either of these is a solution; we have merely proved that *if* there is a solution it is either 5 or -5. Upon substituting these numbers into the given equation, we find that 5 satisfies it while -5 does not. Thus the equation has just one solution, namely $x_1 = 5$.

Whether the solution we obtain is meaningful or not depends upon the kind of number which the unknown must be. Thus, if the unknown represents a number of men, clearly only a positive integer or 0 will suffice. If it represents a length, any positive real number or 0 will do. If it represents a point in the plane, a complex number is allowable.

We shall in the course of this book develop the theory of several different number fields, the rational field, the real field, and the complex field. There are many other number fields besides these, but these are the best known and the most important. The most distinctive property of a number field is that, if a and b are in the field, so are $a + b$, $a - b$, ab, and (provided $b \neq 0$) a/b. In the case of linear equations only these so-called rational operations are involved so that, if the coefficients lie in a field F, so will the solutions. This does not apply in general to quadratic equations, or to those of higher degree.

2. The Linear Equation

The equation

$$ax + b = 0$$

where a and b are numbers of a field F is by no means trivial. Let us divide the discussion into two cases, case I when $a \neq 0$ and case II when $a = 0$. We assume in case I that the equation has a solution x_1 so that

$$ax_1 + b = 0.$$

Since $a \neq 0$, we may divide through by it and obtain $x_1 = -b/a$ as the only candidate for a solution. That this is actually a solution follows from the fact that

$$a\left(\frac{-b}{a}\right) + b = -b + b = 0.$$

In case II we have the equation

$$0 \cdot x + b = 0.$$

Since the product of 0 by every number is 0, it is clear that, if the equation has a solution, it must be true that $b = 0$. If $b = 0$, every number is a solution. Thus in case II there is no solution, or every number is a solution, according as b is not or is 0.

The solution of an equation in one unknown number is based upon the following fundamental law which holds in every field: *A product is equal to* 0 *if and only if one of its factors is equal to* 0. Thus there are three and only three ways in which the equation

$$(x - 2)(x + 3)(x - \sqrt{2}) = 0$$

may be satisfied. If $x = 2$, the first factor is 0; if $x = -3$, the second factor is 0; if $x = \sqrt{2}$, the third factor is 0. Thus the problem of solving a polynomial equation is equivalent to the problem of factoring a polynomial into its linear factors.

In the case of a quadratic polynomial,

$$\begin{aligned} ax^2 + bx + c &= a\left[x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} - \left(\frac{b^2}{4a^2} - \frac{c}{a}\right)\right] \\ &= a\left[\left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right] \\ &= a\left(x + \frac{b}{2a} + \frac{\sqrt{b^2 - 4ac}}{2a}\right)\left(x + \frac{b}{2a} - \frac{\sqrt{b^2 - 4ac}}{2a}\right). \end{aligned}$$

Since $a \neq 0$, the quadratic equation

$$ax^2 + bx + c = 0$$

has two and only two roots, namely

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Exercise 1

Solve the following equations:

1. $(x + 3)(x - 5) = 0$.
2. $(x + 3)(x - 5) = 1$.
3. $(x^2 - 2)(x^2 - 2x - 15) = 0$.
4. $x^2 + 5x + 2 = 0$.
5. $x^2 - 5x + 8 = (x - 3)(x - 2)$.
6. $x^2 + 2x - 8 = (x + 4)(x - 2)$.

7. $\dfrac{x^2 - 7x + 10}{x - 5} = 6.$

8. $\dfrac{x^2 - 7x + 10}{x - 5} = 3.$

9. $\dfrac{x^2 - 7x + 10}{x - 5} = x - 2.$

10. $x - 7 - \sqrt{x - 5} = 0.$

11. $2x + \sqrt{x^2 - 7} = 5.$

12. $\sqrt{x + 5} + \sqrt{x - 4} = 9.$

13. $\sqrt{x + 5} - \sqrt{x - 4} = 9.$

14. $v^2 - 516.17v + 1852.6 = 0.$

15. Solve for x the equation of Guldberg and Waage (chemistry):

$$K(a - x)(b - x) = (c + x)(d + x) \qquad K \neq 1.$$

16. Form an equation having the roots (*a*) 2 and 3, (*b*) $-\frac{1}{2}$ and $\frac{2}{3}$, (*c*) -4.31 and 7.21.

3. The Linear Equation in Several Unknowns

We may consider equations such as

$$2x - 3y - 1 = 0$$

involving two unknown numbers x and y. A *solution* in this case is a pair of numbers as (2, 1) having the property that, when the first number of the pair is substituted for x and the second for y, the equation is satisfied.

An equation of the type

$$ax + by + c = 0$$

ordinarily has infinitely many solutions, for a number of any field in which the coefficients lie can be assigned to one of the unknown symbols x or y and the resulting equation solved for the other unknown. As the student will remember from his course in analytic geometry, every solution corresponds to a point in the plane, and if all the real solutions of such an equation are plotted on a Cartesian graph it will be found that they lie on a straight line. For this reason an equation that involves no term of degree higher than the first and actually has one term of degree 1 is called a *linear equation*. Not every equation of the form

$$ax + by + c = 0$$

is linear, for if $a = b = 0$ there is no solution unless $c = 0$, and every pair of numbers is a solution if $a = b = c = 0$. To indicate that this equation is actually linear, we may write

$$ax + by + c = 0 \qquad (a, b) \neq (0, 0),$$

the second statement indicating that not both a and b are 0.

The equation

$$ax + by + cz + d = 0 \qquad (a, b, c) \neq (0, 0, 0)$$

is said to be linear in the three unknown numbers x, y, and z. A solution consists of a triple of numbers (x_1, y_1, z_1) which, when substituted respectively for x, y, and z into the equation, satisfy it. The equation has infinitely many solutions which constitute a plane in the geometry of three dimensions.

There is no reason why we should stop with three unknowns. For each positive integer n and any field F we may consider the linear equation

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n + c = 0, \quad a_1 \text{ not all } 0 \text{ in } F.$$

A solution consists of an n-tuple of numbers $(p_1, p_2, \cdots, p_n)$ such that, when p_i is substituted into the equation for x_i, the equation is satisfied. There is, strictly speaking, no geometric interpretation for such an equation when $n > 3$ or the field is not real, but we frequently carry over our geometric terminology and say that such an equation represents a plane in n-dimensional space.

4. Equivalence of Equations

Two equations are said to be *equivalent* if every solution of each is a solution of the other. Thus

$$x^2 - 2x - 3 = 0, \qquad 5(x - 3)(x + 1) = 0$$

are equivalent to each other. So also are

$$\sqrt{x^2 - 9} = \tfrac{4}{5}x, \qquad x = 5.$$

So also are

$$2x - 3y - 1 = 0, \qquad y = \tfrac{2}{3}x - \tfrac{1}{3}.$$

Two equivalent equations are frequently considered to be the same equation, for they both impose the same conditions upon the unknown number or numbers, and they have the same graphs. In fact, there is no other reasonable sense in which two equations can be considered to be the same.

In particular, if every term of an equation be multiplied by the same non-zero number, the new equation is equivalent to the original, but we must be certain that the multiplier is not zero.

We should note that this relation of equivalence possesses the characteristic properties of an equivalence relation, namely:

R. Reflexive: Every equation is equivalent to itself.

S. Symmetric: If one equation is equivalent to a second, then the second is equivalent to the first.

T. Transitive: If one equation is equivalent to a second, and the second is equivalent to a third, then the first is equivalent to the third.

5. Linear Systems in Two Unknowns

Often the solution of a problem requires the determination of two numbers which simultaneously satisfy two conditions or equations. Suppose that x and y are to be determined so that

$$\begin{cases} x - 3y + 7 = 0, \\ 2x + y - 7 = 0, \end{cases}$$

both equations holding for the same pair of numbers. By grouping these equations with a brace, we form a linear system of equations and indicate that we are interested only in their common solutions.

A solution, then, of a linear system of equations in two unknowns is a pair of numbers (x_1, y_1) in the given field F containing the coefficients which is a solution of all the equations of the system, x_1 being substituted for x and y_1 for y. Thus (2, 3) is the unique solution of the above system. Two linear systems are *equivalent* if every solution of each system is a solution of the other. The process of solving a linear system consists in replacing the given system successively by equivalent systems until a particularly simple system is reached.

There are three operations by which one may pass from a given system to an equivalent system which are sufficient to solve the system. They are known as the *elementary operations* upon a system of equations. They are of three types:

Type 1. The interchange of two equations.

Type 2. The multiplication of (each term of) an equation by the same non-zero number of F.

Type 3. The addition to the members of one equation of k times the corresponding members of another equation of the system where k is any number of F.

Clearly an operation of type 1 does not alter the solutions of the system, and an operation of type 2 merely replaces an equation by another equation equivalent to it. In considering operations of type 3, we must show that

$$\begin{cases} a_1x + b_1y + c_1 = 0, \\ a_2x + b_2y + c_2 = 0, \end{cases} \qquad \begin{cases} a_1x + b_1y + c_1 = 0, \\ a_2x + b_2y + c_2 + k(a_1x + b_1y + c_1) = 0 \end{cases}$$

are equivalent for every number k. Let (x_1, y_1) denote a solution of the first system. Then

$$a_1x_1 + b_1y_1 + c_1 = 0, \qquad a_2x_1 + b_2y_1 + c_2 = 0$$

and so of course

$$a_2x_1 + b_2y_1 + c_2 + k(a_1x_1 + b_1y_1 + c_1) = 0$$

for every k, and (x_1, y_1) is a solution of the second system.

Conversely, let (x_2, y_2) be a solution of the second system. From the equations

$$a_1x_2 + b_1y_2 + c_1 = 0, \qquad a_2x_2 + b_2y_2 + c_2 + k(a_1x_2 + b_1y_2 + c_1) = 0$$

it follows that

$$a_2x_2 + b_2y_2 + c_2 = 0$$

so that (x_2, y_2) is a solution of the first system also. Since every solution of each system is a solution of the other, the two systems are equivalent.

Example. Solve

$$\begin{cases} x - 3y + 7 = 0, \\ 2x + y - 7 = 0. \end{cases}$$

If we add three times the second equation to the first equation, we obtain the equivalent system

$$\begin{cases} 7x \qquad - 14 = 0, \\ 2x + y - 7 = 0. \end{cases}$$

Now divide the first equation through by 7:

$$\begin{cases} x \qquad - 2 = 0, \\ 2x + y - 7 = 0. \end{cases}$$

Add to the second equation the first equation multiplied by -2:

$$\begin{cases} x - 2 = 0, \\ y - 3 = 0, \end{cases} \quad \text{or} \quad \begin{cases} x = 2, \\ y = 3. \end{cases}$$

We now assert that the linear system has been solved.

6. Intersecting Lines

The geometric interpretation of this process is of some interest. For each real value of k the equation

$$(x - 3y + 7) + k(2x + y - 7) = 0$$

passes through the intersection of the two given lines. As k varies from 0 to 3 the line rotates from the position of $x - 3y + 7 = 0$ about the point (2, 3) until it becomes vertical, namely $x = 2$. Then, as l varies from 0 to -2, the line

$$l(x - 3y + 7) + (2x + y - 7) = 0$$

rotates about the point (2, 3) from the position $2x + y - 7 = 0$ to a

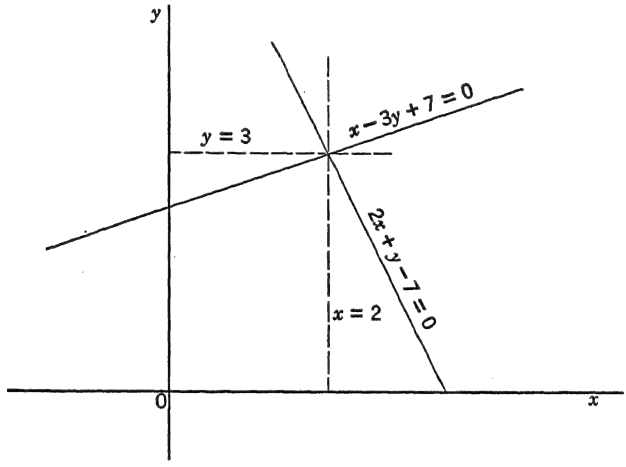

FIG. 1

horizontal position, namely $y = 3$. When the lines have become vertical and horizontal, we assert that the linear system has been solved.

Exercise 2

Solve the following systems of equations:

1. $\begin{cases} 3x - y + 5 = 0, \\ 4x + 3y - 2 = 0. \end{cases}$

2. $\begin{cases} 2x + y = 0, \\ 3x - 2y = 0, \end{cases}$

3. $\begin{cases} 4x - 2y = 0, \\ -6x + 3y = 0. \end{cases}$

4. $\begin{cases} 2x + y - 1 = 0, \\ 3x - 2y + 2 = 0, \\ x - 4y + 2 = 0. \end{cases}$

5. $\begin{cases} x - 2y + 3 = 0, \\ -3x + 6y - 9 = 0, \\ 2x - 4y + 6 = 0. \end{cases}$

6. Two 6-volt batteries, each with an internal resistance of 0.05 ohm, are connected in parallel to a load resistance of 9.0 ohms. How much current flows through the load resistance? By the Kirchhoff laws we have the simultaneous equations

$$9.05I_1 + 9I_2 = 6,$$

$$9I_1 + 9.05I_2 = 6.$$

Find I_1 and I_2.

7. Show that all numbers of the form $a + b\sqrt{2}$ where a and b are rational form a field.

7. Linear Systems in n Unknowns

By the following procedure every linear system of equations with coefficients in any field F can be solved by the use of elementary operations. Suppose that the system is of the form

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= c_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= c_2, \\ \cdots\cdots\cdots\cdots\cdots\cdots & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= c_m, \end{aligned}$$

where all the coefficients and the constant terms lie in a field F.

The *main diagonal* is the sequence of coefficients a_{mn}, $a_{m-1,n-1}$, $a_{m-2,n-2}$, $\cdots$. Thus in Example 2 of this section the main diagonal is $(1, -13, 1)$, while in Example 3 it is $(1, -3, -1)$.

If the coefficient of x_n is 0 in every equation, insert the vanishing equation

$$0 \cdot x_1 + 0 \cdot x_2 + \cdots + 0 \cdot x_n = 0$$

below the other equations. If in some equation the coefficient of x_n is not 0, place one such equation in last position, and divide the equation by this coefficient so that now $a_{mn} = 1$. Now subtract from the ith equation a_{in} times the last equation for $i = 1, 2, \cdots, m - 1$ and obtain a linear system equivalent to the given system of the form

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1,n-1}x_{n-1} &= c_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2,n-1}x_{n-1} &= c_2, \\ \cdots\cdots\cdots\cdots\cdots\cdots & \\ a_{m-1,1}x_1 + a_{m-1,2}x_2 + \cdots + a_{m-1,n-1}x_{n-1} &= c_{m-1}, \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n-1}x_{n-1} + x_n &= c_m. \end{aligned}$$

Now ignore the last equation and work similarly with the equations above it. Each diagonal coefficient can be made 1 unless it is 0 and all

coefficients above it are 0, in which case all the equations are to be moved up one place and a vanishing equation inserted.

No matter how large m is, all left members above the lowest n equations will be made to vanish by this process. If there is an equation whose left member vanishes and whose constant term does not vanish, the given system is inconsistent and has no solution. Otherwise it will have at least one solution.

Now start with the next-to-the-last equation whose diagonal coefficient is 1, and add a multiple of it to the last equation to make the coefficient below it equal to 0. Continue until the canonical form is reached in which

1. Every coefficient above the diagonal is 0.
2. Every diagonal coefficient is either 1 or 0.
3. If a diagonal coefficient is 0, every coefficient of that equation (except possibly the constant term) is 0.
4. If a diagonal coefficient is 1, every coefficient below it is 0.

From this canonical form the general solution of the linear system is immediately obtainable.

Example 1.

$$\begin{cases} 3x - 2y + 4z = 13 \\ 2x + 5y - 3z = -9, \\ 7x + 8y - 2z = -6. \end{cases}$$

$$\begin{cases} 17x + 14y = 1, \\ -\frac{17}{2}x - 7y = 0, \\ -\frac{7}{2}x - 4y + z = 3. \end{cases}$$

$$\begin{cases} 0x = 1, \\ \frac{17}{14}x + y = 0, \\ -\frac{7}{2}x - 4y + z = \frac{5}{2}. \end{cases}$$

The first equation tells us that the system has no solution.

Example 2.

$$\begin{cases} 3x + 4y - 5z = 6, \\ x - 10y + 7z = -2, \\ 3x - 13y + 8z = 0, \\ 2x - 3y + z = 2. \end{cases}$$

$$\begin{cases} 13x - 11y = 16, \\ -13x + 11y = -16, \\ -13x + 11y = -16, \\ 2x - 3y + z = 2. \end{cases}$$

$$\begin{cases} 0 = 0, \\ 0x = 0, \\ -\frac{13}{11}x + y = -\frac{16}{11}, \\ 2x - 3y + z = 2. \end{cases}$$

The equations are consistent, and can be reduced to the canonical form

$$\begin{cases} 0x = 0, \\ -\frac{13}{11}x + y = -\frac{16}{11}, \\ -\frac{17}{11}x + z = -\frac{26}{11}. \end{cases}$$

Clearly x is arbitrary. Let x equal the parameter p. Then the general solution is

$$\begin{cases} x = p, \\ y = -\frac{16}{11} + \frac{13}{11}p, \\ z = -\frac{26}{11} + \frac{17}{11}p, \end{cases}$$

or

$$(x, y, z) = (0, -\tfrac{16}{11}, -\tfrac{26}{11}) + p(1, \tfrac{13}{11}, \tfrac{17}{11}).$$

This yields a solution for every value of p in the field F, and every solution is of this form for some p.

Example 3.

$$\begin{cases} 8x - y - 9z + 3w = 8, \\ 3x - y - 3z + w = 3, \\ 2x + y - 3z + w = 2. \end{cases}$$

This is readily reducible to

$$\begin{cases} 2x - 4y = 2, \\ x - 2y = 1, \\ 2x + y - 3z + w = 2. \end{cases}$$

Since the coefficient of z in the third equation is 0, we move the first

two equations up a position and insert a vanishing equation:

$$\begin{cases} 2x - 4y & = 2, \\ x - 2y & = 1, \\ 0x + 0y + 0z & = 0, \\ 2x + y - 3z + w & = 2, \end{cases}$$

$$\begin{cases} 0x & = 0, \\ -\frac{1}{2}x + y & = -\frac{1}{2}, \\ 0x + 0y + 0z & = 0, \\ 2x + y - 3z + w & = 2. \end{cases}$$

The equations are consistent, and the canonical form is

$$\begin{cases} 0x & = 0, \\ -\frac{1}{2}x + y & = -\frac{1}{2}, \\ 0x + 0y + 0z & = 0, \\ \frac{5}{2}x - 3z + w & = \frac{5}{2}. \end{cases}$$

Since both x and z have diagonal coefficients which are 0, both are arbitrary. The general solution is

$$x = p, \quad y = -\tfrac{1}{2} + \tfrac{1}{2}p, \quad z = q, \quad w = 2\tfrac{1}{2} - \tfrac{5}{2}p + 3q$$

where p and q are parameters, which can be written

$$(x, y, z, w) = (0, -\tfrac{1}{2}, 0, \tfrac{5}{2}) + p(1, \tfrac{1}{2}, 0, -\tfrac{5}{2}) + q(0, 0, 1, 3).$$

In this example the coefficients belong to the rational field, also to the real field, and to the complex field. The question may properly be asked if the totality of solutions is the same under all three assumptions. The answer is no, for, if we are seeking rational solutions, the parameters p and q are restricted to rational values, while in the other two cases they may be real or complex respectively. There are more solutions to this system, then, in the complex field than in the rational field.

It cannot be emphasized too strongly that one must always pass from a system to an equivalent system. Stray equations not incorporated into a system are valueless.

Exercise 3

Find the general solution of each of the following systems of equations:

1. $\begin{cases} x - y - z = 0, \\ x - 2y + z = 6, \\ 2x + y - 3z = 2. \end{cases}$

2. $\begin{cases} x - y - z = 0, \\ 2x - 3y + z = 0, \\ 3x - 2y - 6z = 0. \end{cases}$

3. $\begin{cases} 2x - 3y + z = 0, \\ 4x - 6y + 2z = 0, \\ 10x - 15y + 5z = 0. \end{cases}$

4. $\begin{cases} x + y + z = 4, \\ y + z + w = 0, \\ x + z + w = 4, \\ x + y + 2w = 0. \end{cases}$

5. $\begin{cases} x + y + z + w = 4, \\ x - y + z - w = 2, \\ x + 2y + 2z - w = 0. \end{cases}$

6. $\begin{cases} x + 2y + z + w = 5, \\ 2x + 4y - 3z - 3w = 0, \\ 3x + 6y - 4z - 4w = 1, \\ 2x + 4y - z - w = 4, \\ x + 2y - z - w = 1. \end{cases}$

7. $\begin{cases} 2x + 3y - \frac{5}{2}z + 5w = 2, \\ 3x + 5y - z + 2w = 3, \\ 7x + 11y - 6z + 12w = 7, \\ 3x + 4y - \frac{13}{2}z + 13w = 3. \end{cases}$

8. $\begin{cases} x + 2y + 9z = 0, \\ 2x + 2z = 0, \\ 3x - 2y - 5z = 0. \end{cases}$

9. $\begin{cases} 3x - 2y - w = 7, \\ 2y + 2z + w = 5, \\ x - 2y - 3z - 2w = -1, \\ y + 2z + w = 6. \end{cases}$

10. $\begin{cases} 0.85x + 0.07y + 3.17z = 1.36, \\ 3.72x - 1.21y + 0.87z = 2.23, \\ 0.98x + 2.82y = -3.88. \end{cases}$

11. A problem in electrical networks (N. M. Cooke, *Mathematics for Electricians and Radiomen*, McGraw-Hill, 1942) leads to the system of equations

$$\begin{aligned} 10 - 3I_2 - 4I_4 &= 0, \\ 10 - 2I_1 - 5I_3 &= 0, \\ -3I_2 + 6I_5 + 2I_1 &= 0, \\ -6I_5 - 4I_4 + 5I_3 &= 0, \\ -3I_2 - 4I_4 + 5I_3 + 2I_1 &= 0. \end{aligned}$$

Find I_1, I_2, I_3, I_4, and I_5.

12. If the constant terms in a linear system are all zero, show that there is always a solution.

CHAPTER 2

Rational Solutions

8. Integers

The *rational integers* or *whole numbers*

$$0, \pm 1, \pm 2, \pm 3, \cdots$$

play a basic role in mathematics. They are sometimes merely called *numbers*, and their study the theory of numbers. We shall consider only a few of their more elementary properties.

It is convenient to separate the rational integers into four classes as follows:

1. *Zero.*
2. The *units* 1 and -1, whose reciprocals are rational integers.
3. The *primes* $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \cdots$ which are neither 0 nor units and which cannot be resolved into two factors neither of which is a unit.
4. The *composite numbers* composed of all numbers not in any of the first three classes.

The numbers a and $-a$ are said to be *associated*, since their quotient is a unit.

If a and b are positive integers, there exist two rational integers q and r such that

$$a = bq + r \qquad 0 \leqq r < b.$$

This is nothing more than the division process familiar in arithmetic.

Every positive number a can be written as a polynomial in any other number $b > 1$ with coefficients that are $\geqq 0$ and $< b$. When we write 5387, for instance, we mean

$$5 \cdot 10^3 + 3 \cdot 10^2 + 8 \cdot 10 + 7.$$

If we wish to write this number as a polynomial in powers of 7, we may proceed as follows:

$$5387 = 769 \cdot 7 + 4, \qquad 769 = 109 \cdot 7 + 6,$$

$$109 = 15 \cdot 7 + 4, \qquad 15 = 2 \cdot 7 + 1.$$

Now starting with the last equation and substituting into the one above it, we have

$$15 = 2 \cdot 7 + 1,$$

$$109 = (2 \cdot 7 + 1)7 + 4 = 2 \cdot 7^2 + 7 + 4,$$

$$769 = (2 \cdot 7^2 + 7 + 4)7 + 6 = 2 \cdot 7^3 + 7^2 + 4 \cdot 7 + 6,$$

$$5387 = (2 \cdot 7^3 + 7^2 + 4 \cdot 7 + 6)7 + 4 = 2 \cdot 7^4 + 7^3 + 4 \cdot 7^2 + 6 \cdot 7 + 4$$

$$= (21464)_7.$$

When a number is written as a polynomial in powers of 10 it is called a *decimal.* When it is written in powers of 7 it is called a *septimal.* Thus the decimal $5387 = (5387)_{10}$ is equal to the septimal $(21464)_7$.

There is no other reason why 10 should have been chosen as the base of our number system than that it is of convenient size and we happen to have ten fingers or digits.

The process of changing from one system to another can be carried out as follows:

$$\begin{array}{r|l} 7 & 5387 \\ \hline & 769 + 4 \\ \hline & 109 + 6 \\ \hline & 15 + 4 \\ \hline & 2 + 1 \end{array} \qquad (21464)_7.$$

To pass from a septimal to a decimal we reverse the steps:

$$2 \cdot 7 + 1 = 15,$$

$$15 \cdot 7 + 4 = 109,$$

$$109 \cdot 7 + 6 = 769,$$

$$769 \cdot 7 + 4 = 5387 \qquad (5387)_{10}.$$

Exercise 4

1. Write out all the primes between 0 and 100.
2. Write 3981 in the scale of 5.
3. Express $(2\alpha 9\beta 6)_{12}$ as a decimal, where α denotes 10 and β denotes 11.

4. Write 93871 as a duodecimal (scale of twelve).

5. Write 381572 as a polynomial in powers of 111.

6. If $a = bq + r$, $0 \leqq r < b$, prove that q and r are unique. *Hint.* Set $a = bq_1 + r_1$, and show that $q = q_1$, $r = r_1$.

7. Construct a multiplication table for septimal numbers, and use it to multiply $(21535)_7$ by $(362)_7$. Check your answer by reducing each of these numbers to decimal, multiplying, and changing your answer to a septimal.

8. Write 0.78 as a septimal. *Hint.* First multiply 0.78 by 49.

9. Greatest Common Divisor

If $a = kn$, we say that n *divides* a and write $n|a$. Thus $2|6$ and $3|6$ and also, of course, $6|6$.

If there exists a number d that divides both a and b (i.e., is a common divisor of a and b) and is a multiple of every common divisor of a and b, then d is called a *greatest common divisor* of a and b. The letters g.c.d. stand for greatest common divisor.

Thus, if $a = 540$ and $b = 630$, the common divisors are

$$\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 9, \pm 10, \pm 15, \pm 18, \pm 30, \pm 45, \pm 90.$$

Each of these 24 common divisors is a divisor of 90 and of -90. Thus 90 and -90 are the two greatest common divisors of 540 and 630. We commonly denote the positive g.c.d. of a and b by (a, b).

It should be noted that the word "greatest" means greatest in size or absolute value, not the algebraically greatest, for, as a matter of fact, -90 is the algebraically least common divisor of 540 and 630.

Theorem 1. If $a = bq + r$, *then* $(a, b) = (b, r)$.

To prove this, let $(a, b) = d$, $(b, r) = d_1$. Since d_1 is a common divisor of b and r, it divides $bq + r$ and hence divides a. Thus d_1 is a common divisor of a and b. But d is a g.c.d. of a and b so that $d_1|d$. Now $a - qb = r$ so that by a similar argument $d|d_1$. If

$$d = kd_1, \qquad d_1 = ld,$$

then

$$d = kld.$$

If $b \neq 0$ it follows that $d \neq 0$ so that $kl = 1$. Hence $k = l = \pm 1$, $d = \pm d_1$. But d and d_1 are positive so that $d = d_1$. If $b = 0$, then $a = r$, and the theorem is trivially true.

The following algorithm (process) for finding a g.c.d. of two positive integers is due to Euclid. Let a and b be the numbers, $b \neq 0$. By division we write

$$
\begin{aligned}
a &= bq_1 + r_1 && 0 \leqq r_1 < b,\\
b &= r_1q_2 + r_2 && 0 \leqq r_2 < r_1,\\
r_1 &= r_2q_3 + r_3 && 0 \leqq r_3 < r_2,\\
&\cdots\cdots\cdots && \cdots\cdots\cdots\\
r_{k-2} &= r_{k-1}q_k + r_k && 0 \leqq r_k < r_{k-1},\\
r_{k-1} &= r_kq_{k+1} + 0.
\end{aligned}
$$

In a finite number of steps a remainder $r_{k+1} = 0$ must appear, since a sequence of positive integers

$$b > r_1 > r_2 > r_3 > \cdots > r_{k-1} > r_k > r_{k+1}$$

each of which is less than the preceding must ultimately lead to a remainder of 0. Then by Theorem 1

$$r_k = (r_k, r_{k-1}) = (r_{k-1}, r_{k-2}) = \cdots = (r_3, r_2) = (r_2, r_1) = (r_1, b) = (b, a).$$

Thus the last remainder which is not 0 is the positive g.c.d. of a and b.

It is not evident from the definition of g.c.d. that it always exists. We have now completed the proof of

Theorem 2. Two numbers not both 0 *have a positive g.c.d.*

Two numbers are said to be *relatively prime* if they have 1 for a g.c.d.

Let us find by Euclid's algorithm the positive g.c.d. of $a = 259$ and $b = 161$. We have

$$
\begin{aligned}
259 &= 1\cdot 161 + 98,\\
161 &= 1\cdot 98 + 63,\\
98 &= 1\cdot 63 + 35,\\
63 &= 1\cdot 35 + 28,\\
35 &= 1\cdot 28 + 7,\\
28 &= 4\cdot 7.
\end{aligned}
$$

Hence (259, 161) = 7.

Theorem 3. If $d = (a, b)$, *there exist rational integers* p *and* q *such that*

$$d = pa + qb.$$

The process for the determination of the p and q of the theorem is implicit in the Euclid algorithm, and can be as well explained by an

example as in general notation. Let $a = 259$, $b = 161$. The equations above, written in reverse order, are equivalent to

$$7 = 35 - 1\cdot 28, \qquad 28 = 63 - 1\cdot 35,$$

$$35 = 98 - 1\cdot 63, \qquad 63 = 161 - 1\cdot 98,$$

$$98 = 259 - 1\cdot 161.$$

Thus

$$\begin{aligned} 7 &= 35 - 1(63 - 1\cdot 35) = -63 + 2\cdot 35 \\ &= -63 + 2(98 - 1\cdot 63) = 2\cdot 98 - 3\cdot 63 \\ &= 2\cdot 98 - 3(161 - 1\cdot 98) = -3\cdot 161 + 5\cdot 98 \\ &= -3\cdot 161 + 5(259 - 1\cdot 161) = 5\cdot 259 - 8\cdot 161. \end{aligned}$$

Thus $p = 5$, $q = -8$. The values of p and q are not unique. The process is general.

It is evident that any number k that is representable linearly in terms of a and b must be divisible by (a, b). For, if

$$k = pa + qb,$$

every common divisor of a and b divides k, so that $(a, b)|k$. Hence (a, b) is the smallest positive integer so representable.

The positive g.c.d. of a and b, then, may be defined as a number $d > 0$ for which integers h, k, p, q exist such that

$$a = hd, \qquad b = kd, \qquad d = pa + qb.$$

Theorem 4. If a and b are relatively prime, there exist rational integers p and q such that

$$pa + qb = 1.$$

For, if a and b are relatively prime, their positive g.c.d. is 1.

Theorem 5. (*Euclid.*) *If $a|bc$ and is relatively prime to b, then $a|c$.*

For if a is relatively prime to b, there exist rational integers p and q such that $pa + qb = 1$. Then

$$pac + qbc = c.$$

Since $a|bc$, it divides the left member of the above equation and therefore divides c.

Theorem 6. If p and q are two positive prime numbers, either $p = q$ or $(p, q) = 1$.

Exercise 5

1. Find a g.c.d. of 437 and 95, and express it linearly in terms of these numbers.

2. Do the same with 3766 and 1540.

3. Show that 60 and 91 are relatively prime, and express 1 as a linear combination of these numbers.

4. If $pa + qb = 1$, show that it is also true that $p_1a + q_1b = 1$ where $p_1 = p + kb$, $q_1 = q - ka$ for an arbitrary integer k.

5. Verify that $66 \cdot 17 - 59 \cdot 19 = 1$. Use Problem 4 to find numbers p_1 and q_1, $0 < p_1 < 19$, such that $17p_1 - 19q_1 = 1$. Is it also true that $0 < q_1 < 17$?

6. Find a g.c.d. of 2808 and 1179, and express it linearly in terms of these numbers.

7. If d and d_1 are both g.c.d.'s of a and b, show that $d = \pm d_1$.

8. Show that, if p and q are both positive prime numbers, then $p|q$ implies $p = q$.

9. Using the multiplication table for septimal numbers, find the positive g.c.d. of $(1163)_7$ and $(164)_7$, and express it linearly in terms of the numbers.

10. Show that, if the prime p divides a^n, then p divides a.

10. Unique Factorization

We now come to a basic theorem in arithmetic, namely

Theorem 7. (*Gauss.*) *Every positive integer* > 1 *is uniquely factorable into positive primes.*

It is quite evident that every such integer can be factored into primes in at least one way. For, if a is not a unit or a prime,

$$a = bc, \qquad 1 < b < a, \quad 1 < c < a.$$

Then, if b is not a unit or a prime, we can write

$$b = de, \qquad a = dec, \quad d < b < a, \quad e < b < a,$$

and thus in a finite number of steps we obtain

$$a = p_1p_2 \cdots p_k.$$

The more difficult step is to prove uniqueness. Suppose that

$$a = p_1p_2 \cdots p_k = q_1q_2 \cdots q_l$$

where the p's and the q's are all primes. Since $p_1|q_1q_2 \cdots q_l$, either $p_1|q_1$ and hence $p_1 = q_1$, or $(p_1, q_1) = 1$ by Theorem 6. In the latter case, by Theorem 5, $p_1|q_2 \cdots q_l$. Either $p_1 = q_2$ or $(p_1, q_2) = 1$, in which case $p_1|q_3 \cdots q_l$. Eventually we find that p_1 is equal to one of

the q's, which can be written first and called q_1. Then

$$p_2p_3 \cdots p_k = q_2q_3 \cdots q_l.$$

As before, p_2 is equal to one of the q's, say q_2, and

$$p_3p_4 \cdots p_k = q_3q_4 \cdots q_l.$$

That is, every p_i is equal to some q_i. It is also clear that $k = l$. For, if, for instance, $k < l$, we should have after k steps

$$1 = q_{l-k} \cdots q_l$$

which is not possible, since the q's are primes.

Example 1. Factor, 27300 into its prime factors.

$$\begin{array}{r|l} 2 & 27300 \\ 2 & 13650 \\ 3 & 6825 \\ 5 & 2275 \\ 5 & 455 \\ 7 & 91 \\ & 13 \end{array} \qquad 27300 = 2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 13.$$

The prime 2 is used as a divisor until the quotient is odd, then 3 is used as many times as it will divide, and so on, the primes being taken in order.

A *least common multiple* (l.c.m.) of two numbers a and b is a common multiple of a and b which divides every common multiple of a and b. The positive least common multiple $[a, b]$ is the smallest positive number that is divisible by both a and b.

Example 2. Find (504, 675) and [504, 675].

$$504 = 2^3 \cdot 3^2 \cdot 7 = 2^3 \cdot 3^2 \cdot 5^0 \cdot 7,$$

$$675 = 3^3 \cdot 5^2 = 2^0 \cdot 3^3 \cdot 5^2 \cdot 7^0.$$

Then, selecting the smallest exponent of each prime, we have

$$(504, 675) = 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^0 = 9,$$

and selecting the largest exponent of each prime, we have

$$[504, 675] = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7 = 37800.$$

Exercise 6

1. Write 5390 as a product of prime factors.

2. List all the divisors of 5390.

3. Let $p_1, p_2, \cdots, p_k$ be the prime numbers $\leqq \sqrt{n}$. Show that, if none of these primes divides n, n is a prime number.

4. Prove that 2477 is a prime number.

5. Write 18900 and 2646 as products of powers of primes, and from this form pick out their positive g.c.d. and l.c.m.

6. Show that $(a, b)\cdot[a, b] = ab$.

7. Find all positive integers x, y, and z such that

$$(\tfrac{9}{8})^x(\tfrac{10}{9})^y(\tfrac{16}{15})^z = 2.$$

[This problem arises in the theory of music. Write as an equation in integers, and use Theorem 7.]

11. Integral Roots of Equations

Consider an equation all of whose coefficients are rational integers, such as

$$3x^3 - 4x^2 - 17x + 6 = 0.$$

Suppose that it has an integral root x_1. Then

$$(-3x_1^2 + 4x_1 + 17)x_1 = 6.$$

Since the left member is clearly the product of two integers one of which is x_1, it follows that $x_1 | 6$. This illustrates

Theorem 8. If $f(x) = 0$ has integral coefficients, each integral root is a divisor of the constant term.

For, if we suppose that

$$f(x) = a_0x^n + a_1x^n + \cdots + a_{n-1}x + a_n = 0$$

has an integral root x_1, then it must be true that

$$(-a_0x_1^n - a_1x_1^{n-1} - \cdots - a_{n-1})x_1 = a_n,$$

whence the theorem follows.

Clearly, then, one may determine by trial the integral roots of an equation whose coefficients are integers. It suffices to list all the divisors of the constant term and to substitute these divisors in turn into the equation. If the equation has an integral root, it will be found among these divisors.

A rapid method of substituting a number into a polynomial is as follows. Let the polynomial be

$$f(x) = c_0x^4 + c_1x^3 + c_2x^2 + c_3x + c_4.$$

We form in turn

$$c_0, \quad c_0a + c_1, \quad (c_0a + c_1)a + c_2 = c_0a^2 + c_1a + c_2,$$

$$(c_0a^2 + c_1a + c_2)a + c_3 = c_0a^3 + c_1a^2 + c_2a + c_3,$$

$$(c_0a^3 + c_1a^2 + c_2a + c_3)a + c_4 = c_0a^4 + c_1a^3 + c_2a^2 + c_3a + c_4 = f(a).$$

The work is usually arranged as follows. Let it be required to find $f(2)$ where $f(x) = 3x^4 - 5x^3 - 7x + 13$.

3	−5	0	−7	13	
	6	2	4	−6	2
3	1	2	−3	7	$= f(2)$

If we divide $f(x)$ by $x - a$, we may observe that the coefficients of the partial quotient are c_0, $c_0a + c_1$, $c_0a^2 + c_1a + c_2$, and $c_0a^3 + c_1a^2 + c_2a + c_3$ and that the remainder is $f(a)$. Thus in our example

$$3x^4 - 5x^3 - 7x + 13 = (3x^3 + x^2 + 2x - 3)(x - 2) + 7.$$

A similar result holds for polynomials of degree n and will be proved later (§ 22).

Example 1. Find all integral roots of

$$f(x) = x^4 + 4x^3 + 8x^2 + 8x + 3 = 0.$$

The only divisors of the constant term 3 are ± 1 and ± 3. Obviously $f(1)$ and $f(3)$ are positive numbers so that 1 and 3 are not roots.

1	4	8	8	3	
	−1	−3	−5	−3	−1
1	3	5	3	0	$= f(-1)$.

Since $f(-1) = 0$, -1 is a root.

1	4	8	8	3	
	−3	−3	−15	21	−3
1	1	5	−7	24	$= f(-3)$.

Then -3 is not a root.

When the constant term has many divisors the method just illustrated is laborious, and the following refinement, due to Newton, is a great time saver. Suppose that the coefficients of

$$f(x) = c_0x^4 + c_1x^3 + c_2x^2 + c_3x + c_4$$

are integers. If x_1 is an integral root $\neq 0$, then c_4/x_1 is an integer and

$$-c_0x_1^3 - c_1x_1^2 - c_2x_1 - c_3 = c_4/x_1.$$

Then

$$c_4/x_1 + c_3 = (-c_0x_1^2 - c_1x_1 - c_2)x_1$$

is an integer which we may call m_1. Clearly $x_1 | m_1$. Then

$$m_1/x_1 + c_2 = (-c_0x_1 - c_1)x_1 = m_2$$

is also divisible by x_1. Again

$$m_2/x_1 + c_1 = -c_0x_1 = m_3$$

is divisible by x_1, and

$$m_3/x_1 + c_0 = 0.$$

If a divisor x_1 of c_4 fails to satisfy one of these conditions, it cannot be a root of $f(x) = 0$.

Example 2. Find the integral roots of $x^3 - x^2 - 14x + 24 = 0$.

The divisors of 24 are ± 1, ± 2, ± 3, ± 4, ± 6, ± 8, ± 12, and ± 24. The numbers ± 1 are easily eliminated by trial. We have 14 remaining possibilities.

$$c_3 = 24, \quad c_2 = -14, \quad c_1 = -1, \quad c_0 = 1.$$

$$m_1 = c_3/x_1 - 14, \quad m_2 = m_1/x_1 - 1, \quad m_3 = m_2/x_1 + 1.$$

x_1	c_3/x_1	m_1	m_1/x_1	m_2	m_2/x_1	m_3
2	12	−2	−1	−2	−1	0
3	8	−6	−2	−3	−1	0
4	6	−8	−2	−3		
6	4	−10				
8	3	−11				
12	2	−12	−1	−2		
24	1	−13				
−2	−12	−26	13	12	−6	
−3	−8	−22				
−4	−6	−20	5	4	−1	0
−6	−4	−18	3	2		
−8	−3	−17				
−12	−2	−16				
−24	−1	−15				

As soon as a non-integral quotient is obtained, such as $m_2/4$, this value of x_1 is eliminated. Only those values that go through to yield 0 in the last column are roots. In this case the integral roots are 2, 3, and -4.

Exercise 7

Find the integral roots, if any, of the following equations:

1. $x^3 + x^2 - 10x + 8 = 0$.
2. $x^3 - 3x^2 + x - 20 = 0$.
3. $x^3 + 3x^2 - 10x - 24 = 0$.
4. $x^4 - 3x^3 - 7x^2 + 27x - 18 = 0$.
5. $x^4 + 2x^3 - 4x^2 - 5x - 6 = 0$.
6. $x^4 - 2x^3 - 12x^2 - 10x + 68 = 0$.
7. $x^4 - 3x^2 + 10x - 6 = 0$.
8. $x^4 - 15x^3 + 63x^2 - 62x + 48 = 0$.
9. $x^5 - 8x^4 + 18x^3 - 18x^2 + 17x - 10 = 0$.
10. Determine all integers k so that $x^3 + 8x^2 + kx + 6 = 0$ shall have an integral root.
11. Let $c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n = 0$ have integral coefficients. If there exists a common divisor d of the coefficients $c_0, c_1, \cdots, c_{n-1}$ that does not divide c_n, show that the equation has no integral root.

12. Bounds for the Roots

Clearly an equation all of whose coefficients are $\geqq 0$ (and at least one of them is > 0) cannot have a positive root, since the substitution of a positive number for the unknown yields a number not 0. A similar argument can, with a little ingenuity, be made to yield an upper bound for the roots of any equation. Thus let

$$f(x) = 3x^3 - 4x^2 - 17x + 6 = x^2(x - 4) + x(2x^2 - 17) + 6 = 0.$$

This will surely be positive for all values of x such that

$$x - 4 \geqq 0, \qquad 2x^2 - 17 \geqq 0.$$

If $x \geqq 4$, both inequalities are satisfied, so that the equation can have no root as large as 4. Thus 4 is an upper bound for the roots.

Furthermore

$$-f(-x) = 3x^3 + 4x^2 - 17x - 6 = x(3x^2 - 17) + 2(2x^2 - 3) = 0$$

has as its roots the negatives of the roots of $f(x) = 0$, so that, if a is an upper bound for the roots of $-f(-x) = 0$, then $-a$ is a lower bound for the roots of $f(x) = 0$. Clearly $\sqrt{17/3} = 2.38$ is such a bound for our equation, so that the real roots of $f(x) = 0$ lie between -2.38 and 4.

Example 1. Find bounds for the roots of $x^3 - x^2 - 14x + 24 = 0$.

This may be written $x(x^2 - x - 14) + 24 = 0$. The expression in

parentheses will be positive for

$$x > \frac{1 + \sqrt{57}}{2} = 4.28.$$

Also $-f(-x) = x(x^2 - 14) + (x^2 - 24) = 0$, from which we obtain the lower bound $-\sqrt{24} = -4.899$ for the given equation.

Example 2. Find upper and lower bounds for the roots of

$$4x^5 - 16x^4 + 9x^3 + 35x^2 - 51x + 18 = 0.$$

This may be grouped

$$4x^4(x - 4) + 9x^3 + x(35x - 51) + 18 = 0,$$

so that 4 is an upper bound. Then

$$-f(-x) = x^2(4x^3 - 35) + x(16x^3 - 51) + 9(x^3 - 2) = 0,$$

from which it is clear that $\sqrt[3]{35/4} = 2.061$ is an upper bound. Thus the roots of the given equation lie between -2.061 and 4.

If a satisfactory bound is not at once evident, the following procedure will help. If the leading coefficient of $f(x)$ is positive, let c be a number for which $f(c) > 0$, and write

$$f(x) = (x - c) \cdot q(x) + f(c).$$

If b is an upper bound for the roots of $q(x) = 0$, then the larger of the two numbers b and c is an upper bound for the roots of $f(x) = 0$.

Example 3. Find an upper bound for the roots of

$$f(x) = x^4 - 2x^3 - 3x^2 - x + 5 = 0.$$

Since $f(3) > 0$, write

$$f(x) = (x - 3)(x^3 + x^2 - 1) + 2.$$

If $x \geqq 1$, $x^3 + x^2 - 1 > 0$, and if $x \geqq 3$, $x - 3 \geqq 0$. Thus 3 is an upper bound.

Exercise 8

Find upper and lower bounds for the roots of

1. $x^4 - 2x^3 + x^2 - 3x + 1 = 0.$
2. $x^4 - 3x^2 + 18x - 20 = 0.$
3. $x^4 - x^3 - 5x^2 + 8x - 9 = 0.$
4. $x^5 + 3x^4 + x^3 - 8x^2 - 51x + 18 = 0.$

5. $x^4 + 4x^3 - 34x^2 - 76x + 105 = 0$.
6. $x^6 - x^5 - x^4 - x^3 - x^2 - x - 1 = 0$.

Find the integral roots of 7 and 8:

7. $x^5 - 41x^3 - 84x^2 + 148x + 336 = 0$.
8. $x^8 - 39x^6 + 399x^4 - 1261x^2 + 900 = 0$.
9. Let $f(x) = x^n + c_1x^{n-1} + \cdots + c_n = 0$. Let p be a prime dividing each integral coefficient $c_1, c_2, \cdots, c_n$. Show that an integral root of $f(x) = 0$ must be divisible by p.
10. Use Problem 9 to find the integral roots of

$$x^4 + 2x^3 - 6x^2 - 38x + 68 = 0.$$

13. Rational Roots

If $f(x) = 0$ is an equation with rational coefficients, we may multiply through by the least common denominator of the coefficients and thus obtain an equivalent equation all of whose coefficients are rational integers.

Theorem 9. If the equation

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

with integral coefficients has a rational root $x_1 = p/q$, $(p, q) = 1$, *then* $p|a_n$ *and* $q|a_0$.

For, if p/q is a root,

$$a_0\frac{p^n}{q^n} + a_1\frac{p^{n-1}}{q^{n-1}} + \cdots + a_{n-1}\frac{p}{q} + a_n = 0,$$

$$a_0p^n + a_1p^{n-1}q + \cdots + a_{n-1}pq^{n-1} + a_nq^n = 0.$$

This may be written in the form

$$a_0p^n = -(a_1p^{n-1} + \cdots + a_{n-1}pq^{n-2} + a_nq^{n-1})q.$$

Clearly $q|a_0p^n$ and, since q is prime to p, $q|a_0$ by Theorem 5. Similarly

$$a_nq^n = -(a_0p^{n-1} + a_1p^{n-2}q + \cdots + a_{n-1}q^{n-1})p$$

so that $p|a_nq^n$ and, by Theorem 5, $p|a_n$.

Example 1. Find the rational roots of

$$6x^3 - x^2 - 19x - 6 = 0.$$

The only possible rational roots are of the form p/q where p is a

divisor of -6 and q is a divisor of the leading coefficient 6. The possibilities are

$$\pm 1,\ \pm 2,\ \pm 3,\ \pm 6,\ \pm\tfrac{1}{2},\ \pm\tfrac{1}{3},\ \pm\tfrac{1}{6},\ \pm\tfrac{2}{3},\ \pm\tfrac{3}{2}.$$

The equation may be written

$$f(x) = x(x^2 - 1) + x(4x^2 - 19) + x^3 - 6 = 0$$

so that $\sqrt{19/4} = 2.18$ is an upper bound for the roots. Also

$$-f(-x) = x(6x^2 - 19) + x^2 + 6 = 0$$

has 1.78 as an upper bound. Thus the roots of $f(x) = 0$ lie between -1.78 and 2.18. The possibilities that remain are

$$\pm 1,\ 2,\ \pm\tfrac{1}{2},\ \pm\tfrac{1}{3},\ \pm\tfrac{1}{6},\ \pm\tfrac{2}{3},\ \pm\tfrac{3}{2}.$$

On trial we find that 2, $-\frac{1}{3}$, and $-\frac{3}{2}$ are the rational roots.

The problem of finding the rational roots of an equation with integral coefficients may be reduced to that of finding the integral roots of a related equation and then, after determining bounds, applying the method of Newton. If the equation is

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0,$$

the substitution $a_0x = y$ will lead to an equation in y with integral coefficients whose leading coefficient is 1. Sometimes a smaller number than a_0 will suffice.

Example 2. Find the rational roots of

$$4x^5 - 16x^4 + 9x^3 + 35x^2 - 51x + 18 = 0.$$

The leading coefficient $4 = 2^2$ becomes a fifth power on multiplication by 8. The equation is equivalent to

$$(2x)^5 - 8(2x)^4 + 9(2x)^3 + 70(2x)^2 - 204(2x) + 144 = 0.$$

If we let $2x = y$, this becomes

$$y^5 - 8y^4 + 9y^3 + 70y^2 - 204y + 144 = 0.$$

An upper bound is 8, and a lower bound is -4.122. The only possible integral roots are ± 1, ± 2, ± 3, ± 4, 6. Newton's method shows that 3 and 4 are the only integral roots of this equation so that $\frac{3}{2}$ and 2 are the only rational roots of the given equation.

Exercise 9

Find the rational roots of

1. $3x^3 - 26x^2 + 34x - 12 = 0$.
2. $4x^4 - 13x^2 + 9 = 0$.
3. $x^2 + 5x + 1 = 0$.
4. $9x^4 - 56x^3 + 57x^2 + 98x - 24 = 0$.
5. $24x^3 - 20x^2 + 7x - 1 = 0$. *Hint.* Let $x = 1/y$.
6. $6x^4 - 7x^3 + 6x^2 - 1 = 0$.
7. For what integral values of k does $x^2 + kx + 1 = 0$ have a rational root?
8. Find all integral values of b for which $x^3 + bx^2 + 3x + 2 = 0$ has a rational root.
9. Show that $x^n - 1 = 0$ has just two rational roots when n is even and only one rational root when n is odd.
10. Show that $\sqrt{2}$ is not a rational number. And, more generally, show that, if a is an integer, $\sqrt{a}$ is either an integer or it is not rational.

CHAPTER

3

Polynomials

14. Rings and Fields

At this point it will be necessary to give more exact definitions of some of our concepts. A set of elements $a, b, c, \cdots$ form a *ring* provided

1. The sum $a + b$ exists in the set.
2. The associative law of addition holds:

$$(a + b) + c = a + (b + c).$$

3. The commutative law of addition holds:

$$a + b = b + a.$$

4. The set contains 0: For every a

$$a + 0 = a.$$

5. For every a there is a ^{-}a in the set such that

$$a + {}^{-}a = 0.$$

1′. The product ab exists in the set.
2′. The associative law of multiplication holds:

$$(ab)c = a(bc).$$

6. The distributive laws hold:

$$a(b + c) = ab + ac, \qquad (b + c)a = ba + ca.$$

The rings which are of most importance are those called *commutative rings with unit element*. They have the additional properties

3′. The commutative law of multiplication holds:

$$ab = ba.$$

4′. The set contains the unit element 1 such that for every a

$$a \cdot 1 = a.$$

The prototype of the ring is the set of rational integers. They form, in fact, a commutative ring with unit element. The even integers form a commutative ring which, however, does not contain a unit element.

A *field* is a commutative ring with unit element which has one more property, namely:

5′. Every element a except 0 has an inverse a^{-1} such that

$$a \cdot a^{-1} = 1.$$

The concept of field is one of the most important concepts in algebra. The set of all rational numbers—i.e., numbers of the form p/q where p and q are integers—constitutes the rational field. The numbers which are limits of sequences of rational numbers (see Chapter 4) constitute the real field. All numbers of the form $a + ib$ where a and b are real and $i^2 = -1$ constitute the complex field (see Chapter 5).

While these are the best-known fields, there are infinitely many others. Thus all rational functions of x with rational coefficients constitute a field. All numbers of the form $a + b\sqrt{2}$ where a and b are rational constitute a field. In fact, for every fixed integer m which is not a square, $a + b\sqrt{m}$ constitute a field. Right here we have infinitely many fields, and we have scarcely scratched the surface.

15. Degree

An expression such as

$$4x^3 + \tfrac{1}{2}x^2 + \sqrt{2}x - 6$$

which is a sum of distinct non-negative integral powers of x, each multiplied by a number of a certain field (the real field in this case), is called a *polynomial over* the field in the indeterminate x. We may write

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n.$$

The polynomial is of degree n if $a_0 \neq 0$. The *degree* is the exponent of the highest power of x which does not vanish. A quadratic polynomial such as $2x^2 - 5x + \frac{1}{2}$ is of degree 2, a linear polynomial is of degree 1, a mere number is of degree 0 provided the number is not itself 0. The number 0 (which may be thought of as a polynomial all of whose coefficients are 0, i.e., the vanishing polynomial) has no degree. Since 0 is the only polynomial that has no degree, this property characterizes it.

Two polynomials are *equal* if and only if their difference is the 0

polynomial. Thus the two polynomials

$$a_0x^3 + a_1x^2 + a_2x + a_3, \qquad b_1x^2 + b_2x + b_3$$

are equal if and only if

$$a_0x^3 + (a_1 - b_1)x^2 + (a_2 - b_2)x + a_3 - b_3 = 0.$$

This means that

$$a_0 = 0, \qquad a_1 - b_1 = 0, \qquad a_2 - b_2 = 0, \qquad a_3 - b_3 = 0$$

so that we may say, in general, that two polynomials are equal if and only if coefficients of corresponding powers of x are equal.

The three concepts of *variable*, *indeterminate*, and *unknown number* should be distinguished. A variable represents all the numbers on its range. An indeterminate * does not represent a number. If x is a variable, then $x^2 - 5x + 6$ is 0 when $x = 2$ or 3. If x is an indeterminate, $x^2 - 5x + 6$ is simply not 0. This approach is more satisfactory than the older attitude of distinguishing between "conditionally equal to 0" and "identically equal to 0."

The product of two polynomials

$$f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m, \qquad g(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n,$$

is a polynomial

$$f(x) \cdot g(x) = a_0b_0x^{m+n} + \cdots + a_mb_n.$$

If $f(x)$ is of degree m so that $a_0 \neq 0$ and if $g(x)$ is of degree n so that $b_0 \neq 0$, then clearly $a_0b_0 \neq 0$ so that $f(x) \cdot g(x)$ is of degree $m + n$. Thus we have established

Theorem 10. The degree of the product of two non-vanishing polynomials is equal to the sum of their degrees.

If either of $f(x)$ or $g(x)$ is the vanishing polynomial, each coefficient of $f(x) \cdot g(x)$ will be 0 so that this product will vanish. On the other hand, if both $f(x)$ and $g(x)$ are non-vanishing, each will have a degree so that, by Theorem 10, the product will have a degree and hence will be non-vanishing. We have proved.

Theorem 11. A product of polynomials vanishes if and only if one of the factors vanishes.

* For an exact definition of indeterminate see C. C. MacDuffee, *Introduction to Abstract Algebra*, Wiley, pp. 158–161.

16. Polynomials with Rational Coefficients

There is a close parallelism between the rational integers and polynomials with rational coefficients, which we can exhibit by separating the polynomials into four classes as we separated the rational integers in § 8:

1. The zero polynomial.
2. The rational numbers with 0 omitted, i.e., the polynomials of degree 0.
3. The irreducible polynomials.
4. All other polynomials.

The principal difference between the rational integers and the rational polynomials is in the second class. There are but two integers, namely 1 and -1, whose reciprocals are also integers. A polynomial will have a reciprocal if it is of degree 0, so that every rational number except 0, considered as a polynomial, is a unit. There are infinitely many unit polynomials.

Two polynomials are said to be *associated* if their quotient is a unit polynomial. Thus

$$-3(x^2 - 5), \qquad \tfrac{1}{2}(x^2 - 5)$$

are associated.

A polynomial is said to be *irreducible* over the rational numbers if it cannot be represented as a product of two polynomials with rational coefficients, neither of which is a unit polynomial. Thus

$$\tfrac{7}{2}x^2 - 14 = \tfrac{7}{2}(x - 2)(x + 2)$$

is reducible, while $x^2 - 14$ is irreducible over the rational numbers. The latter is reducible over the real field, however.

Theorem 12. If $f(x)$ and $g(x)$ are two polynomials over a field F, the latter non-vanishing, there exist uniquely two polynomials $q(x)$ and $r(x)$ over F, the latter either the zero polynomial or of degree less than the degree of $g(x)$, such that

$$f(x) = q(x) \cdot g(x) + r(x).$$

The process for finding the polynomials $q(x)$ and $r(x)$ is familiar to every student under the name of "long division" although no division is involved. Thus let

$$f(x) = 4x^3 - 2x^2 + 5x + 3, \qquad g(x) = 2x^2 + x - 1.$$

Note that the leading coefficient of $f(x)$, namely $4x^3$, is obtained by

multiplying the leading coefficient of $g(x)$, namely $2x^2$, by $2x$. Hence the difference

$$f(x) - 2x \cdot g(x) = -4x^2 + 7x + 3$$

is of degree less than the degree of $f(x)$. Since $-4x^2/2x^2 = -2$, we form

$$f(x) - 2x \cdot g(x) + 2g(x) = 9x + 1.$$

Since this remainder is of degree less than the degree of $g(x)$, we can continue no further. Then

$$f(x) = 4x^3 - 2x^2 + 5x + 3 = (2x - 2) \cdot g(x) + 9x + 1.$$

The method is perfectly general. If $f(x)$ is of lower degree than $g(x)$, let $q(x) = 0$ and $r(x) = f(x)$.

To show that $q(x)$ and $r(x)$ are unique, let us assume that we also have

$$f(x) = q_1(x) \cdot g(x) + r_1(x)$$

where $r_1(x)$ is 0 or of degree less than the degree m of $g(x)$. Then we should have

$$[q(x) - q_1(x)] \cdot g(x) = r_1(x) - r(x).$$

Unless $q(x) - q_1(x)$ vanishes, it has a degree $\geqq 0$ so that the left-hand side of the equation is of degree $\geqq m$. The right-hand side, however, is of degree $< m$. Hence each side vanishes and

$$q(x) = q_1(x), \qquad r(x) = r_1(x).$$

Theorem 12 becomes particularly simple when $g(x)$ is of the form $x - a$. In fact, the process of § 11 gives both $q(x)$ and $r(x)$, the latter being a number since $x - a$ is linear. To see that this is so, it is sufficient to divide

$$c_0x^4 + c_1x^3 + c_2x^2 + c_3x + c_4$$

by $x - a$ by ordinary division and to observe that the coefficients of the quotient are the numbers

$$c_0, \quad c_0a + c_1, \quad c_0a^2 + c_1a + c_2, \quad \text{etc.}$$

Example. Let $f(x) = x^5 - 4x^3 + 2x^2 - 5x - 8$, $a = 3$.

1	0	−4	2	−5	−8	3
	3	9	15	51	138	
1	3	5	17	46	130	

Hence $f(x) = (x^4 + 3x^3 + 5x^2 + 17x + 46)(x - 3) + 130$.

Exercise 10

1. What is the degree of $x^4 + 5x^2 + 1$ considered as a polynomial in x? What is its degree considered as a polynomial in x^2?

2. If $f(x) = x^4 + 4x^3 + 4x^2 + 7x + 13$ and $g(x) = x + 2$, find the $q(x)$ and $r(x)$ of Theorem 12.

3. Do the same for $f(x) = x^5 - 5x^4 + 6x^3 - 8x^2 + 31x - 21$ and $g(x) = x - 3$.

4. Do the same for $f(x) = x^5 - \frac{1}{5}x^4 + \frac{2}{25}x - \frac{3}{125}$, $g(x) = x - \frac{1}{5}$.

5. Do the same for $f(x) = 2x^5 - 3x^4 + 5x^2 - 6$, $g(x) = x^2 + x + 3$.

6. Do the same for $f(x) = x^5 - 3x^4 - 39x^3 + 104x^2 + 108x + 145$, $g(x) = x^2 - 2x - 24$.

7. Prove that a polynomial of degree 2 or 3 with rational coefficients is irreducible over the rational numbers unless the equation obtained by setting this polynomial equal to 0 has a rational root.

8. Determine whether $x^3 - x^2 - x - 2$ is reducible or irreducible.

9. Show that $x^3 - 6x^2 + 9x + 2$ is rationally irreducible.

10. Express $x^4 + 3x^2 + 2x + 3$ as a product of two quadratic factors each with integral coefficients. [The factors must be of the form $x^2 + bx + c$ where $c = \pm 1$ or ± 3.]

17. Polynomials in Powers of a Given Polynomial

Theorem 13. Let $f(x)$ and $g(x)$ be two polynomials, $g(x)$ of degree $m \geqq 1$. There exist unique polynomials $c_0(x)$, $c_1(x)$, $\cdots$, $c_k(x)$, each 0 or of degree $< m$, such that

$$f(x) = c_0(x) + c_1(x)\cdot g(x) + c_2(x)\cdot[g(x)]^2 + \cdots + c_k(x)\cdot[g(x)]^k.$$

Let $f(x) = q(x)\cdot g(x) + c_0(x)$ where $c_0(x)$ is 0 or of degree $< m$. Similarly let

$$\begin{aligned}
g(x) &= q_1(x)\cdot g(x) + c_1(x),\\
q_1(x) &= q_2(x)\cdot g(x) + c_2(x),\\
&\cdots\cdots\cdots\cdots\cdots\\
q_{k-2}(x) &= q_{k-1}(x)\cdot g(x) + c_{k-1}(x),\\
q_{k-1}(x) &= c_k(x).
\end{aligned}$$

Eventually for some k, $q_{k-1}(x)$ will be of degree $< m$, for the degrees of the q's form a sequence of decreasing positive integers. Then

$$\begin{aligned}
f(x) &= [q_1(x)\cdot g(x) + c_1(x)]\cdot g(x) + c_0(x)\\
&= q_1(x)\cdot[g(x)]^2 + c_1(x)\cdot g(x) + c_0(x) = \cdots\\
&= c_k(x)\cdot[g(x)]^k + \cdots + c_1(x)\cdot g(x) + c_0(x) \qquad c_k(x) \not\equiv 0.
\end{aligned}$$

These coefficients are unique. For suppose that we also have

$$f(x) = d_l(x)[g(x)]^l + \cdots + d_1(x)\cdot g(x) + d_0(x) \qquad d_l(x) \not\equiv 0.$$

Upon subtracting these two forms of $f(x)$, we have

$$\{d_l(x)[g(x)]^{l-1} - c_k(x)[g(x)]^{k-1} + \cdots + d_1(x) - c_1(x)\}g(x) = c_0(x) - d_0(x).$$

The left side is 0 or of degree $\geqq m$; the right side is 0 or of degree $< m$. Hence $d_0(x) = c_0(x)$, and

$$\{d_l(x)\cdot[g(x)]^{l-2} - c_k(x)\cdot[g(x)]^{k-2} + \cdots + d_2(x) - c_2(x)\}g(x) = c_1(x) - d_1(x)$$

As before, $d_1(x) = c_1(x)$. We continue until (if $l > k$)

$$d_l(x)\cdot[g(x)]^{l-k-1} + \cdots + d_{k+1} = 0.$$

Then each of the remaining d's is zero so that it must have been true that $l = k$.

The process is particularly simple when the divisor is of the form $x - a$. In this case Taylor's theorem can be used:

$$f(x) = f(a) + f'(a)\cdot(x-a) + \frac{1}{2}f''(a)\cdot(x-a)^2 + \cdots + \frac{1}{n!}f^{(n)}(a)\cdot(x-a)^n.$$

Since $f(x)$ is a polynomial, the expansion is finite.

It is even more rapid to use the method of detached coefficients.

Example 1. Express $f(x) = x^3 + 7x^2 + 10x - 1$ as a polynomial in powers of $x - 0.09$.

If we use § 11 to perform the divisions, we have

1	7	10	−1	
	0.09	0.6381	0.957429	0.09
1	7.09	10.6381	−0.042571	
	0.09	0.6462		
1	7.18	11.2843		
	0.09			
1	7.27			

$$f(x) = (x - 0.09)^3 + 7.27(x - 0.09)^2 + 11.2843(x - 0.09) - 0.042571.$$

The geometric significance of this process is of interest. The graphs of

$$y = x^3 + 7x^2 + 10x - 1,$$

$$y = x^3 + 7.27x^2 + 11.2843x - 0.042571$$

are identical except that the second is shifted 0.09 unit to the left; or, if we prefer, the new y axis is 0.09 unit to the right of the old y axis.

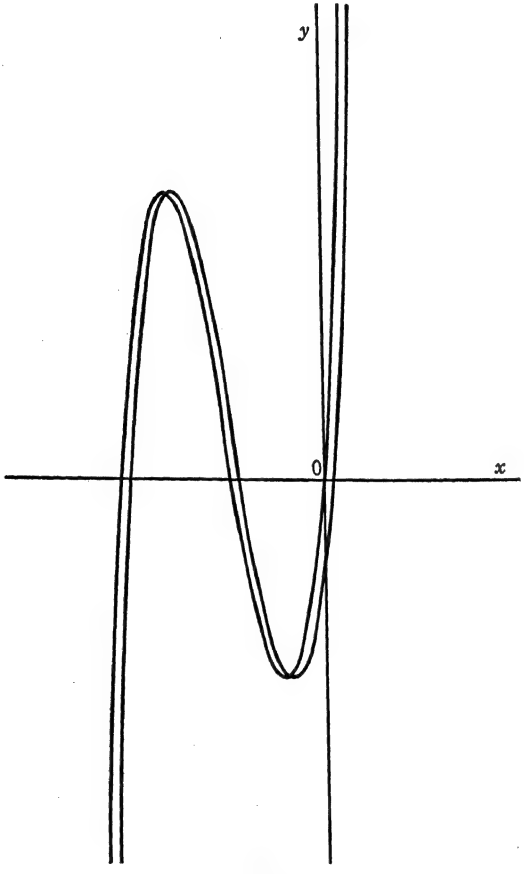

FIG. 2

By such a shift, the polynomial

$$y = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$$

may be written in *reduced form*

$$y = u^n + b_2u^{n-2} + \cdots + b_n$$

with the next to highest term missing. In fact, if we set $u = x + a_1/n$, or $x = u - a_1/n$, we achieve the reduction. For

$$\begin{aligned} y &= (u - a_1/n)^n + a_1(u - a_1/n)^{n-1} + \cdots \\ &= u^n - a_1u^{n-1} + \cdots + a_1u^{n-1} + \cdots \\ &= u^n + \cdots \end{aligned}$$

where the dots represent only terms of degree less than $n - 1$ in u.

Example 2. Find the reduced form of $x^3 + 12x^2 + 30x + 5$.

Here $a_1/n = 4$.

$$\begin{array}{llll|l} 1 & 12 & 30 & 5 & \\ & -4 & -32 & 8 & -4 \\ \hline 1 & 8 & -2 & 13 & \\ & -4 & -16 & & \\ \hline 1 & 4 & -18 & & \\ & -4 & & & \\ \hline 1 & 0 & & & \end{array}$$

The reduced form is $u^3 - 18u + 13$, $u = x + 4$.

Exercise 11

1. By the method used to prove Theorem 13, express $x^3 + 2x^2 - 23x - 60$ as a polynomial in powers of $x - 2$.

2. Solve Problem 1 by Taylor's theorem.

3. Solve Problem 1 using division by detached coefficients.

4. By the method used to prove Theorem 13, express $x^5 - 10x^3 + 2x^2 + 17x + 6$ as a polynomial in powers of $x + 2$.

5. Solve Problem 4 by Taylor's theorem.

6. Solve Problem 4 using division by detached coefficients.

7. Given $f(x) = x^4 - 8x^3 - 34x^2 - 76x + 105$. Use division by detached coefficients to calculate $f(-2)$, $f'(-2)$, $f''(-2)$ and $f'''(-2)$. Check by taking the derivatives.

8. Express $x^3 - 2x - 5$ as a polynomial in powers of $x - 2.1$.

9. Express $x^4 - 5x^3 + 7x^2 - 17x + 11$ as a polynomial in powers of $x - 4$.

10. Express $x^4 - 7x^3 + 6x^2 + 7x - 11$ as a polynomial in powers of $x + 1.11$.

11. Express $2x^7 + x^6 + 7x^5 + 7x^3 - x^2 - 3x + 3$ as a polynomial in powers of $x^2 + 1$.

12. Express $2x^8 + x^7 + 5x^6 + x^5 + 6x^4 + 9x^3 + x^2 + 3x + 7$ as a polynomial in powers of $x^3 + x + 1$.

13. Let $f(x)$ be expressed as a polynomial in powers of $g(x)$, and let $c_0(x)$ be the last coefficient in this expansion. Let a be a number such that $g(a) = 0$. Show that $f(a) = c_0(a)$.

18. The Greatest Common Divisor

A polynomial $d(x)$ is said to be a *greatest common divisor* (g.c.d.) of two polynomials $f(x)$ and $g(x)$ if $d(x)|f(x)$ and $d(x)|g(x)$, [i.e., if $d(x)$ is a common divisor of $f(x)$ and $g(x)$] and if every common divisor of $f(x)$ and $g(x)$ divides $d(x)$. We shall show (Theorem 15) that every two polynomials not both zero have infinitely many greatest common divisors.

Theorem 14. If $f(x) = q(x) \cdot g(x) + r(x)$, then every g.c.d. of $f(x)$ and $g(x)$ is a g.c.d. of $g(x)$ and $r(x)$, and conversely.

The proof is like that of Theorem 1. Every common divisor of $f(x)$ and $g(x)$ divides $r(x)$, and every common divisor of $g(x)$ and $r(x)$ divides $f(x)$.

There is a Euclid algorithm for the determination of the greatest common divisor of two polynomials very similar to the Euclid algorithm for the determination of the greatest common divisor of two integers. Let

$$\begin{aligned} f(x) &= q_1(x) \cdot g(x) + r_1(x), \\ g(x) &= q_2(x) \cdot r_1(x) + r_2(x), \\ r_1(x) &= q_3(x) \cdot r_2(x) + r_3(x), \\ &\cdots\cdots\cdots\cdots \\ r_{k-1}(x) &= q_{k+1}(x) \cdot r_k(x), \end{aligned}$$

each remainder being either 0 or of degree less than the degree of the divisor. In a finite number of steps a remainder 0 will be obtained. The last non-zero remainder is the g.c.d. of $f(x)$ and $g(x)$.

If $f(x) = g(x) = 0$, their g.c.d. is 0 by definition. We have thus proved

Corollary 14. Every two polynomials $f(x)$ and $g(x)$ have a greatest common divisor $d(x)$.

Theorem 15. If $d(x)$ is a g.c.d. of $f(x)$ and $g(x)$, and if k is a non-zero number, then $kd(x)$ is also a g.c.d. Conversely, if $d(x)$ and $d_1(x)$ are two g.c.d.'s, there exists a number $k \neq 0$ such that $d_1(x) = kd(x)$.

The direct theorem is obvious. If $d(x)$ and $d_1(x)$ are two g.c.d.'s of $f(x)$ and $g(x)$, $d(x)|d_1(x)$ and $d_1(x)|d(x)$ by definition of g.c.d. Thus $d_1(x) = k(x)\cdot d(x)$, $d(x) = l(x)\cdot d_1(x) = l(x)\cdot k(x)\cdot d(x)$. If $d(x) \neq 0$, $l(x)\cdot k(x) = 1$ so that $k(x) = k$ and $l(x) = l$ are numbers not 0. If $d(x) = 0$, then $f(x) = g(x) = 0$ so that $d_1(x) = 0$ and k is arbitrary.

Since a non-zero constant is a unit, the theorem states that the g.c.d. is unique up to a unit factor.

Theorem 16. If $d(x)$ is a g.c.d. of $f(x)$ and $g(x)$, there exist polynomials $s(x)$ and $t(x)$ such that

$$d(x) = s(x)\cdot f(x) + t(x)\cdot g(x).$$

The proof follows from the Euclid algorithm in a manner similar to the proof of Theorem 3.

19. Unique Factorization

We shall say that $f(x)$ and $g(x)$ are *relatively prime* polynomials if their g.c.d.'s are non-zero constants. Then 1 is a g.c.d.

Theorem 17. If $f(x)$ is of degree $m > 0$ and $g(x)$ is of degree $n > 0$, and if $f(x)$ and $g(x)$ are relatively prime, then there exists a polynomial $s(x)$ of degree $< n$ and a polynomial $t(x)$ of degree $< m$ such that

$$1 = s(x)\cdot f(x) + t(x)\cdot g(x).$$

By Theorem 16 there exist polynomials $s_1(x)$ and $t_1(x)$ such that

$$1 = s_1(x)\cdot f(x) + t_1(x)\cdot g(x).$$

We may write

$$s_1(x) = q_1(x)\cdot g(x) + s(x),$$

$$t_1(x) = q_2(x)\cdot f(x) + t(x)$$

where $s(x)$ is 0 or of degree $< n$ and $t(x)$ is 0 or of degree $< m$. Then

$$1 - s(x)\cdot f(x) - t(x)\cdot g(x) = [q_1(x) + q_2(x)]\cdot f(x)\cdot g(x).$$

Unless $q_1(x) + q_2(x) = 0$, the right side is of degree $\geqq m + n$ while the left side is of degree $< m + n$, which is impossible. Thus

$$1 = s(x)\cdot f(x) + t(x)\cdot g(x).$$

Both $s(x)$ and $t(x)$ have degrees unless $f(x)$ or $g(x)$ is a constant, for otherwise, if $s(x) = 0$ or $t(x) = 0$, the right side could not be of degree 0.

Theorem 18. If $f(x)$ and $g(x)$ are relatively prime polynomials and if $g(x)|f(x)\cdot h(x)$, then $g(x)|h(x)$.

From Theorem 17 we have

$$1 = s(x)\cdot f(x) + t(x)\cdot g(x),$$

$$h(x) = s(x)\cdot f(x)\cdot h(x) + t(x)\cdot g(x)\cdot h(x).$$

Since $g(x)$ divides both terms on the right, $g(x)\big|h(x)$.

Theorem 19. Every polynomial $f(x)$ is representable in the form

$$f(x) = [p_1(x)]^{\alpha_1}[p_2(x)]^{\alpha_2}\cdots[p_k(x)]^{\alpha_k}$$

where $p_1(x)$, $p_2(x)$, $\cdots$, $p_k(x)$ are distinct irreducible polynomials. The representation is unique except for the order of the factors and that the irreducible factors can be replaced by associates.

The proof follows from Theorem 18 in the same way that the proof of Theorem 7 follows from Theorem 5.

Note that the two factorizations

$$x^2 - 1 = (x + 1)(x - 1) = (2x + 2)(\tfrac{1}{2}x - \tfrac{1}{2})$$

are the same except that the unit 2 has been removed from the second factor and multiplied into the first. These two factorizations are associated.

Two factorizations of the same polynomial may be quite different if they are not carried to the irreducible factors. Thus

$$\begin{aligned} x^6 - 1 &= (x^3 - 1)(x^3 + 1) \\ &= (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1), \\ x^6 - 1 &= (x^2 - 1)(x^4 + x^2 + 1) \\ &= (x - 1)(x + 1)(x^2 + 1 + x)(x^2 + 1 - x). \end{aligned}$$

Exercise 12

1. Find a greatest common divisor of

$$f(x) = 4x^3 - 17x^2 + 11x + 5, \qquad g(x) = 2x^3 - 3x^2 - 11x - 3.$$

2. Find a greatest common divisor of

$$f(x) = x^5 + 2x^4 - 5x^3 - 3x^2 - 6x + 15,$$

$$g(x) = 2x^4 + 5x^3 - 11x^2 - 11x + 15.$$

3. Find a greatest common divisor of

$$f(x) = x^4 - x^3 - 3x^2 + x + 2, \qquad g(x) = 2x^4 + 3x^3 - x^2 - 3x - 1.$$

4. Find a greatest common divisor of

$$f(x) = \tfrac{1}{3}x^4 + \tfrac{2}{5}x^3 - \tfrac{1}{12}x - \tfrac{1}{10}, \qquad g(x) = \tfrac{1}{6}x^3 - \tfrac{2}{15}x^2 + \tfrac{19}{15}x + 2.$$

5. Show that $x^2 + x + 2$ and $x^2 - x$ are relatively prime, and find polynomials $s(x)$ and $t(x)$ such that

$$s(x)\cdot(x^2 + x + 2) + t(x)\cdot(x^2 - x) = 1.$$

6. Find a greatest common divisor of

$$f(x) = x^4 + x^2 + 1, \qquad g(x) = x^2 - x + 1$$

and express it in the form $s(x)\cdot f(x) + t(x)\cdot g(x)$.

7. Factor $x^8 - 1$ into its irreducible factors.

8. Given $f(x) = x^2 - x + 1$, $g(x) = x^2 + 1$. Verify that

$$(x^2 + x + 1)\cdot f(x) - x^2\cdot g(x) = 1,$$

and find $s(x)$ and $t(x)$ each of degree 1 such that

$$s(x)\cdot f(x) + t(x)\cdot g(x) = 1.$$

9. Prove that the $s(x)$ and $t(x)$ of Theorem 17 are unique. *Hint.* Assume another representation with $s_1(x)$ and $t_1(x)$. Then

$$[s(x) - s_1(x)]\cdot f(x) = [t_1(x) - t(x)]\cdot g(x).$$

Since $f(x)$ is prime to $g(x)$, use Theorem 18.

20. Partial Fractions

The quotient of two polynomials, such as

$$\frac{x^3 + 5x + 7}{2x^2 - 5}$$

is called a *rational function*, or a *rational fraction*. The numerator may be any polynomial, while the denominator may be any polynomial except 0. When the denominator is a non-zero constant, the rational fraction is a polynomial. Two rational functions $f_1(x)/g_1(x)$ and $f_2(x)/g_2(x)$ are defined to be equal if $f_1(x)\cdot g_2(x) = f_2(x)\cdot g_1(x)$.

We recall from elementary algebra that the sum, difference, product, and quotient (except by 0) of two rational functions is again a rational function.

The *degree* of a rational function is defined to be the degree of the numerator minus the degree of the denominator. The fraction is called *proper* if its degree is a negative integer; otherwise it is called improper.

Theorem 20. Every rational fraction is uniquely expressible as a sum of a polynomial and a proper fraction.

For, since $g(x) \neq 0$, we may determine by Theorem 12 two polynomials $q(x)$ and $r(x)$ such that

$$f(x) = q(x) \cdot g(x) + r(x) \tag{1}$$

where $r(x) = 0$ or is of lower degree than $g(x)$. Then

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}. \tag{2}$$

Conversely (2) implies (1). By Theorem 12, $q(x)$ and $r(x)$ are unique.

Theorem 21. If $f_1(x)/g_1(x)$ and $f_2(x)/g_2(x)$ are proper, so is their sum.

Let $f_1(x)$ be of degree m_1, $g_1(x)$ of degree n_1, $f_2(x)$ of degree m_2, $g_2(x)$ of degree n_2, $m_1 < n_1$, $m_2 < n_2$. The sum is

$$\frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} = \frac{f_1(x) \cdot g_2(x) + f_2(x) \cdot g_1(x)}{g_1(x) \cdot g_2(x)}.$$

The denominator is of degree $n_1 + n_2$ while the numerator is of degree $\leqq$ the greater of $m_1 + n_2$, $m_2 + n_1$, each of which is less than $n_1 + n_2$.

Theorem 22. If $f(x)/g_1(x) \cdot g_2(x)$ is proper and if $g_1(x)$ and $g_2(x)$ are relatively prime, the fraction can be uniquely expressed

$$\frac{f(x)}{g_1(x) \cdot g_2(x)} = \frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)}$$

where $f_1(x)/g_1(x)$ and $f_2(x)/g_2(x)$ are proper.

Since $g_1(x)$ and $g_2(x)$ are relatively prime, there exist by Theorem 17 polynomials $s_1(x)$ and $s_2(x)$ such that

$$1 = s_2(x) \cdot g_2(x) + s_1(x) \cdot g_1(x).$$

Then

$$\frac{f(x)}{g_1(x) \cdot g_2(x)} = \frac{s_2(x) \cdot f(x)}{g_1(x)} + \frac{s_1(x) \cdot f(x)}{g_2(x)}.$$

These fractions may not be proper, and so by Theorem 20 we determine polynomials $p_1(x)$, $p_2(x)$, $f_1(x)$, and $f_2(x)$ such that

$$\frac{s_2(x) \cdot f(x)}{g_1(x)} = p_1(x) + \frac{f_1(x)}{g_1(x)}, \qquad \frac{s_1(x) \cdot f(x)}{g_2(x)} = p_2(x) + \frac{f_2(x)}{g_2(x)},$$

where $f_1(x)/g_1(x)$ and $f_2(x)/g_2(x)$ are proper. Then

$$\frac{f(x)}{g_1(x) \cdot g_2(x)} = \frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} + p_1(x) + p_2(x).$$

Since the sum of the two proper fractions is proper by Theorem 21, and the left member is proper, and the representation of a rational fraction as the sum of a polynomial and a proper fraction is unique by Theorem 20, we must have

$$p_1(x) + p_2(x) = 0$$

so that the statement in the theorem is established.

To show the uniqueness, let us assume that there are two representations

$$\frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} = \frac{h_1(x)}{g_1(x)} + \frac{h_2(x)}{g_2(x)}$$

where all four fractions are proper. Then

$$f_1(x)\cdot g_2(x) + f_2(x)\cdot g_1(x) = h_1(x)\cdot g_2(x) + h_2(x)\cdot g_1(x),$$

$$[f_1(x) - h_1(x)]\cdot g_2(x) = [h_2(x) - f_2(x)]\cdot g_1(x).$$

Since $g_1(x)$ and $g_2(x)$ are relatively prime, $g_2(x) | h_2(x) - f_2(x)$ by Theorem 18. Since the degree of $h_2(x) - f_2(x)$ is less than the degree of $g_2(x)$, it follows that $h_2(x) - f_2(x) = 0$. Hence also $f_1(x) - h_1(x) = 0$. This concludes the proof.

Let $g(x)$ be written

$$g(x) = [p_1(x)]^{\alpha_1}[p_2(x)]^{\alpha_2} \cdots [p_k(x)]^{\alpha_k}$$

where the $p_i(x)$ are irreducible. The prime powers $[p_i(x)]^{\alpha_i}$ are relatively prime in pairs, so that by a repeated application of Theorem 22 we can write the proper fraction

$$\frac{f(x)}{g(x)} = \sum_{i=1}^{k} \frac{f_i(x)}{[p_i(x)]^{\alpha_i}}$$

where each of the summands is proper. Now by Theorem 13 we write

$$f_i(x) = c_{i0}(x) + c_{i1}(x)\cdot p_i(x) + c_{i2}(x)[p_i(x)]^2 + \cdots$$

as a polynomial in powers of $p_i(x)$ where each coefficient $c_{ij}(x)$ is 0 or of degree less than the degree of $p_i(x)$. Thus

$$\frac{f(x)}{g(x)} = \sum_{i=1}^{k} \frac{c_{i0}(x)}{[p_i(x)]^{\alpha_i}} + \frac{c_{i1}(x)}{[p_i(x)]^{\alpha_i - 1}} + \frac{c_{i2}(x)}{[p_i(x)]^{\alpha_i - 2}} + \cdots.$$

This establishes the theory of partial fractions, which in its practical applications is known to all students of integral calculus. The actual determination of the coefficients is usually easier by the method of undetermined coefficients, but in most texts on calculus the proof of the existence of the partial fraction decomposition is not given. That is,

the student has no prior guarantee that the system of equations for the coefficients that he sets up will have a solution in all cases. That fact we have now established.

Exercise 13

1*a*. Write

$$\frac{2x^4 - 5x^3 + 2x^2 - 5x + 1}{x(x^2 + x + 1)}$$

as the sum of a polynomial and a proper fraction by division.

1*b*. Find polynomials $s(x)$ and $t(x)$ such that

$$s(x)\cdot x + t(x)\cdot(x^2 + x + 1) = 1.$$

1*c*. Express each of

$$\frac{-(x+1)(7x^2+2x+1)}{x^2+x+1}, \qquad \frac{7x^2+2x+1}{x}$$

as the sum of a polynomial and a proper fraction, and find their sum.

1*d*. What is the representation of the original fraction as a sum of a polynomial and two proper fractions each with irreducible denominator?

2. Use undetermined coefficients to solve Problem 1. Assume

$$\frac{7x^2+2x+1}{x(x^2+x+1)} = \frac{A}{x} + \frac{Bx+C}{x^2+x+1},$$

$$7x^2 + 2x + 1 = A(x^2 + x + 1) + (Bx + C)x,$$

whence

$$A + B = 7, \qquad A + C = 2, \qquad A = 1.$$

3. Use the method of the first problem to express

$$\frac{2x}{(x-1)^2(x+2)}$$

as a sum of two proper fractions.

4. Use the method of the second problem to express

$$\frac{6x^3 - x^2}{(2x^2 - x + 8)^2}$$

as a sum of two proper fractions with linear numerators.

5. Break into partial fractions

$$\frac{x^7 + 3x^6 + 18x^5 + 31x^4 + 90x^3 + 75x^2 + 127x + 1}{(x^2 + x + 5)^3}.$$

21. Zeros of Rational Functions

The indeterminate x is a polynomial, not a number, although it is added and multiplied by the same rules that apply to numbers. If $f(x)$ is a polynomial and we substitute a number a for x, we call the re-

sulting number $f(a)$, if it exists, a *functional value*, but it is not always permissible to substitute a number for x, as we shall see.

The polynomial $f(x) = x^2 - 5x + 6$ in the indeterminate x is not 0, for not all of its coefficients are 0. Yet $f(3) = 0$, and also $f(2) = 0$. We call 2 and 3 *zeros* of the polynomial $f(x)$, or *roots* or *solutions* of the equation $f(x) = 0$.

The existence of these zeros makes it impossible to substitute certain numbers into a rational function. Thus

$$f(x) = \frac{x + 1}{x^2 - 5x + 6}$$

has functional values for all numbers except 2 and 3, but $f(2)$ and $f(3)$ do not exist, for we may not divide by 0.

For the indeterminate x it is true that

$$\frac{x^2 - 5x + 6}{x - 2} = x - 3$$

but, if we attempt to substitute 2 for x into this equation, we obtain -1 on the right, while substitution into the left member is impossible.

Theorem 23. If $r_1(x)$ and $r_2(x)$ are rational functions and if

$$r_1(x) = r_2(x),$$

then $r_1(a) = r_2(a)$ for every number a which is not a zero of the denominator of either function.

If

$$r_1(x) = \frac{f_1(x)}{g_1(x)}, \qquad r_2(x) = \frac{f_2(x)}{g_2(x)}$$

where neither $g_1(x)$ nor $g_2(x)$ is the zero polynomial, then $r_1(x) = r_2(x)$ implies

$$f_1(x) \cdot g_2(x) - f_2(x) \cdot g_1(x) = 0.$$

This expression is a polynomial equation, every coefficient of which is 0. Hence for every number a

$$f_1(a) \cdot g_2(a) - f_2(a) \cdot g_1(a) = 0.$$

Now, if a is not a zero of $g_1(x)$ or of $g_2(x)$, then $g_1(a) \cdot g_2(a) \neq 0$, and

$$\frac{f_1(a)}{g_1(a)} = \frac{f_2(a)}{g_2(a)},$$

as was to be proved.

If a is a zero of $g_1(x)$ or of $g_2(x)$, clearly $r_1(a)$ or $r_2(a)$ does not exist.

Corollary 23. A zero of a rational function

$$r(x) = f(x)/g(x)$$

is a number which is a zero of the numerator $f(x)$ and which is not a zero of the denominator $g(x)$.

Thus to solve the equation

$$r(x) = f(x)/g(x) = 0,$$

we must first remove all common factors from numerator and denominator and then set the numerator equal to 0. The zeros of this polynomial are then the zeros of $r(x)$.

Example. Solve

$$\frac{x+3}{x^2-1} + \frac{x-3}{x^2-x} + \frac{x+2}{x^2+x} = 0.$$

The least common denominator is $x(x^2-1)$ so that upon adding the fractions we have

$$\frac{x^2+3x}{x(x^2-1)} + \frac{x^2-2x-3}{x(x^2-1)} + \frac{x^2+x-2}{x(x^2-1)} = \frac{3x^2+2x-5}{x(x^2-1)} = 0.$$

The g.c.d. of numerator and denominator is $x-1$. Upon removing it, we have

$$\frac{3x+5}{x(x+1)} = 0.$$

Since the numerator and denominator are now relatively prime, this equation is equivalent to

$$3x + 5 = 0$$

whose only solution is $x = -5/3$.

Exercise 14

Solve each of the following equations:

1. $1 - \dfrac{x^2}{x-1} = \dfrac{1}{1-x} - 6.$

2. $\dfrac{3x-1}{2x-1} - \dfrac{4x-2}{3x-1} = \dfrac{1}{6}.$

3. $\dfrac{30+6x}{x+1} + \dfrac{60+8x}{x+3} = 14 + \dfrac{48}{x+1}.$

(First reduce each term to the sum of a polynomial and a proper fraction.)

4. $\dfrac{x+4}{x-4}+\dfrac{x-2}{x-3}=6\frac{1}{3}$.

5. $\dfrac{x+1}{x+2}+\dfrac{x-1}{x-2}=\dfrac{2x-1}{x-1}$.

6. $\dfrac{3}{x}+\dfrac{6}{x-1}-\dfrac{x+5}{x(x-1)}=0$.

7. $\dfrac{x+1}{x(x-2)}-\dfrac{1}{2x-2}+\dfrac{1}{2x}=0$.

8. $\dfrac{x+3}{4(x+2)(3x-1)}+\dfrac{2x+1}{3(3x-1)(x+4)}-\dfrac{17x+7}{6(x+4)(x+2)}=0$.

22. The Remainder Theorem

In every number field, such as the rational, real, or complex numbers, a product of two numbers is 0 if and only if one of the numbers is 0. Thus, if we have an equation such as

$$2(x-3)(x+5)=0,$$

we know that this product can be made 0 only by one of the factors becoming 0. Clearly $2 \neq 0$, so that the only possibilities are $x-3=0$ or $x+5=0$. Thus there are just two solutions, $x=3$ and $x=-5$. Thus solving an equation $f(x)=0$ is the same problem as factoring the polynomial $f(x)$. There is basically only one "method" of solving such an equation.

Theorem 24. The Remainder Theorem. The remainder obtained upon dividing the polynomial $f(x)$ by $x-a$ is the number $f(a)$.

By Theorem 12 the polynomial $f(x)$ can be written

$$f(x)=q(x)\cdot(x-a)+r$$

where $r=0$ or is of degree 0—that is, r is free of x. By Theorem 23

$$f(a)=q(a)\cdot(a-a)+r=r.$$

From this theorem we have an important corollary:

Corollary 24. The Factor Theorem. If a is a zero of the polynomial $f(x)$, then $f(x)$ is divisible by $x-a$ without a remainder.

For, if $f(a)=r=0$, then

$$f(x)=q(x)\cdot(x-a).$$

Theorem 25. An equation $f(x)=0$ of degree n with coefficients in a field F can have no more than n roots in F.

By Theorem 19 the polynomial $f(x)$ can be uniquely written in the form

$$f(x)=[p_1(x)]^{\alpha_1}[p_2(x)]^{\alpha_2}\cdots[p_k(x)]^{\alpha_k}$$

where the $p_i(x)$ are irreducible over F. If $p_i(x)$ is of degree d_i, then $\alpha_1 d_1+\alpha_2 d_2+\cdots+\alpha_k d_k=n$. By the factor theorem $f(a)=0$ only

if one of these irreducible factors $p_i(x)$ is of the form $x - a$. Obviously the number of such roots a is $\leqq n$.

23. Multiple Roots

According to our definition of root or solution, it is scarcely sensible to speak of a multiple root. For a is or is not a root of $f(x) = 0$ according as $f(a) = 0$ or $f(a) \neq 0$. But it is sensible to speak of a multiple zero of a polynomial. Let

$$f(x) = (x - a)^k \cdot g(x) \qquad g(a) \neq 0.$$

Then we say that a is a zero of $f(x)$ of *multiplicity* k. A zero of multiplicity one is called a *simple* zero. If $f(a) \neq 0$, we may call a a zero of $f(x)$ of multiplicity 0. It is common although slightly uncritical usage to call a zero of $f(x)$ of multiplicity k a root of $f(x) = 0$ of multiplicity k.

Theorem 26. If a is a zero of the polynomial $f(x)$ of multiplicity $k \geqq 1$, then a is a zero of the derived function $f'(x)$ of multiplicity $k - 1$.

Let

$$f(x) = (x - a)^k \cdot g(x) \qquad g(a) \neq 0.$$

We know from the calculus that

$$\begin{aligned} f'(x) &= k(x - a)^{k-1} \cdot g(x) + (x - a)^k \cdot g'(x) \\ &= (x - a)^{k-1}[kg(x) + (x - a) \cdot g'(x)]. \end{aligned}$$

This shows that a is a zero of $f'(x)$ of multiplicity at least $k - 1$. If the multiplicity were greater than $k - 1$, $x - a$ would be a divisor of

$$kg(x) + (x - a) \cdot g'(x).$$

Since it is obviously a divisor of the second term, it would have to be a divisor of $g(x)$ so that we should have $g(a) = 0$, contrary to assumption.

Corollary 26. If a is a zero of $f(x)$ of multiplicity k, then a is a zero of the greatest common divisor $d(x)$ of $f(x)$ and $f'(x)$ of multiplicity $k - 1$.

Theorem 27. Let $d(x)$ be a greatest common divisor of $f(x)$ and $f'(x)$. Then $f(x)/d(x)$ is a polynomial which has the same zeros as $f(x)$, but each one is simple.

Thus by means of the Euclid algorithm for determining a g.c.d., a method that involves only the rational operations, an equation $f(x) = 0$ can be replaced by another equation $f(x)/d(x) = 0$ which has the same roots as $f(x) = 0$ and where the polynomial $f(x)/d(x)$ has only simple zeros.

Corollary 27. If a polynomial $f(x)$ has rational coefficients and is rationally irreducible, it has only simple zeros.

For in this case every divisor is a constant, and in particular the g.c.d. $d(x)$ of $f(x)$ and $f'(x)$ is a constant.

Exercise 15

1. Find whether $x^3 + x^2 - x - 1$ has multiple zeros.
2. Find the multiple zeros of $x^4 - 2x^3 - 11x^2 + 12x + 36$.
3. Find an equation with simple roots having the same distinct roots as $x^3 + 5x^2 + 8x + 4 = 0$. Use Theorem 27.
4. Find an equation with simple roots having the same distinct roots as $x^5 - x^4 + 3x^3 + x^2 + 4 = 0$.
5. For what value or values of q will $x^3 - 3x + q$ have a multiple zero?
6. Show that $x^3 + px + q = 0$ will have a multiple root if and only if $-4p^3 - 27q^2 = 0$.
7. Show that $x^n - a^n$ is exactly divisible by $x - a$ for every positive integer n.
8. Find the remainder obtained upon dividing $x^7 - a^7$ by $x - a$; by $x + a$.
9. Find the remainder obtained upon dividing $x^{10} - 1$ by $x^2 - a$.
10. Prove: Let $p(x)$ be rationally irreducible and let $[p(x)]^r$, $r > 0$, be the highest power of $p(x)$ that divides $f(x)$. Then $[p(x)]^{r-1}$ is the highest power of $p(x)$ that divides $f'(x)$. Pattern the proof on that of Theorem 26.

CHAPTER

4

Real Roots

24. The Real Numbers

Until now we have discussed mainly the rational numbers. A *real number* is a number that is defined by a convergent sequence of rational numbers. We recall the definition from the calculus. A sequence

$$a_0, a_1, a_2, \cdots, a_p, \cdots$$

is called *regular* and defines a real number if for every rational number ϵ there exists a positive integer N_ϵ such that, for p and $q > N_\epsilon$,

$$|a_p - a_q| < \epsilon.$$

An infinite decimal defines such a sequence. Thus $\sqrt{2}$ is defined by the successive approximations

$$1.4,\ 1.41,\ 1.414,\ 1.4142,\ 1.41421,\ 1.414213,\ \cdots.$$

It can be shown that every real number not 0 can be written as a positive or negative finite or infinite decimal.

We must re-examine the definition of solution of an equation. Let $f(x)$ be a polynomial with rational (or real) coefficients. We seek a regular sequence

$$x_0, x_1, x_2, \cdots, x_p, \cdots$$

with the property that for every rational (or real) number ϵ there exists a positive integer N_ϵ such that for $p > N_\epsilon$

$$|f(x_p)| < \epsilon.$$

For instance, let $f(x) = x^2 - 2$. Then

$|f(1.4)| = 0.04$, $|f(1.41)| = 0.0119$,

$|f(1.414)| = 0.000704$, $|f(1.4142)| = 0.00003836$,

$|f(1.41421)| = 0.0000100759$, $|f(1.414213)| = 0.000001590631$.

Thus, for $\epsilon = 0.000011$, $p = 4$, $x_4 = 1.41421$.

A function $y = f(x)$ is said to be *continuous* at the point $x = a$ if

$$(1)\ f(a) \text{ exists}, \qquad (2)\ \lim_{x \to a} f(x) = f(a), \qquad (3)\ \lim_{x \to a} f(x) = f(a).$$

The symbol $x \rightarrow a$ means that x approaches a through values greater than a, i.e., from the right, while $x \rightarrow a$ means that x approaches a from the left.

A function is said to be *continuous in an interval* if it is continuous for every value of x in that interval.

A little consideration will convince the student that this definition of continuity is consistent with our intuitive concept, namely that the curve $y = f(x)$ can be drawn in an interval in which it is continuous as a single piece without lifting the pencil from the paper.

Theorem 28. A polynomial with real coefficients is continuous for every finite value of x.

We recall from the calculus that the limit of a sum of two functions is equal to the sum of their limits, and that the limit of the product of two functions is equal to the product of their limits. Clearly the limit of a constant is that constant. Let

$$f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n.$$

Then as x approaches a from either side

$$\begin{aligned}
\lim f(x) &= \lim (c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n) \\
&= \lim (c_0x^n) + \lim (c_1x^{n-1}) + \cdots + \lim (c_{n-1}x) + c_n \\
&= c_0 \lim (x^n) + c_1 \lim (x^{n-1}) + \cdots + c_{n-1} \lim x + c_n \\
&= c_0(\lim x)^n + c_1(\lim x)^{n-1} + \cdots + c_{n-1} \lim x + c_n \\
&= c_0a^n + c_1a^{n-1} + \cdots + c_{n-1}a + c_n = f(a).
\end{aligned}$$

This limit clearly exists for every finite a so that the curve extends infinitely far to the left and to the right. Since there is one and only one value of $f(a)$ for every a, every vertical line cuts the curve just once.

In the remainder of this chapter a polynomial will mean a polynomial with real coefficients.

25. Polynomial Curves

Since the derivative of a polynomial is a polynomial, it is continuous. In fact, the derivatives of all orders are continuous. The continuity of the first derivative indicates that the slope of $y = f(x)$ changes continuously, i.e., that the curve is smooth. The continuity of the first

two derivatives show that the curvature changes continuously. Since the real zeros of the first derivative give the x co-ordinates of the points with horizontal tangents, a polynomial curve of degree n can have at most $n - 1$ maxima and minima. Since the real zeros of the second derivative determine the inflection points, the curve can have at most $n - 2$ of these.

The two following theorems are now intuitively obvious.

Theorem 29. If $f(x)$ is a polynomial and $f(a)$ and $f(b)$ have opposite signs, there are an odd number of values x_1 of x between a and b such that $f(x_1) = 0$, counting a multiple root as many times as its multiplicity.

Theorem 30. Rolle's Theorem. If $f(x)$ is a polynomial and $f(a) = f(b) = 0$, there is at least one value x_1 of x between a and b such that $f'(x_1) = 0$.

Example. As an illustration of Theorem 29 let us consider the equation $y = f(x) = x^5 - 3$. Since $f(1) = -2$ and $f(2) = 27$, there is at least one root of $f(x) = 0$ between 1 and 2, presumably nearer to 1 than to 2. We find $f(1.5) = 4.6$ so that 1.5 is too large. Since $f(1.2) = -0.512$, 1.2 is too small. We now have

$$f(1.25) = 0.05, \qquad f(1.24) = -0.07,$$
$$f(1.245) = -0.009, \qquad f(1.246) = 0.003,$$
$$f(1.2455) = -0.0029, \qquad f(1.2458) = 0.0005,$$
$$f(1.2457) = -0.0005.$$

Hence 1.2457 is an approximate solution of the equation. The exact solution is an irrational real number, the limit of a sequence whose early terms are

$$1, 2, 1.5, 1.2, 1.25, 1.24, 1.245, 1.246, 1.2455, 1.2458, 1.2457 \cdots.$$

Exercise 16

1. Treat the equation $y = f(x) = x^2 - 7$ in a manner suggested by the illustrative example above.

2. If $y = f(x)$ is a polynomial, show that the curvature function

$$k(x) = \frac{f''(x)}{[1 + (f'(x))^2]^{3/2}}$$

is a continuous function of x for all finite values of x.

3. Show that $y = x^3 - 2x^2 - 3x$ cuts the x axis at $x = 0$ and at $x = 3$. Find all values of x between 0 and 3 at which dy/dx vanishes.

4. Show that the maximum or minimum point of the parabola $y = ax^2 + bx + c$ has an x co-ordinate which is the average of the x co-ordinates of the intercepts.

5. Show that the inflection point of the cubic parabola $y = ax^3 + bx^2 + cx + d$ is on the line joining the maximum and minimum points (if they are real) and is halfway between them. *Hint.* Choose axes so that the curve has the equation

$$y' = a'x'^3 + c'x'.$$

6. Show that every polynomial equation of odd degree with real coefficients has at least one real root.

26. Graphing

In finding the real roots of a polynomial equation such as

$$f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n = 0$$

whose coefficients are real, the graph of $y = f(x)$ is of great help, for the real roots of the equation are the points where the graph crosses

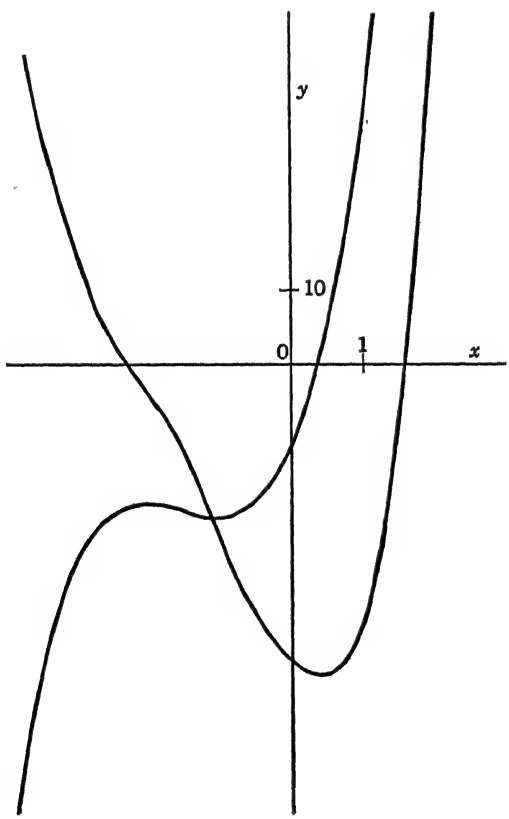

FIG. 3

or touches the x axis. An adequate graph is not always easy to plot, but the methods of the calculus used with a little care and patience will yield a graph from which first approximations to the root can be read. Then algebraic methods to be described later will refine these approximate roots to any desired degree of accuracy. Frequently only part of the graph need be plotted.

Example. Plot the graph of $y = f(x) = x^4 + 6x^3 + 12x^2 - 11x - 41$.

We note that

$$f'(x) = 4x^3 + 18x^2 + 24x - 11,$$

$$f''(x) = 12x^2 + 36x + 24$$

$$= 12(x + 1)(x + 2).$$

The roots of $f''(x) = 0$ are at -1 and -2 so that the equation $f'(x) = y$ has a minimum at $(-1, -21)$ and a maximum at $(-2, -19)$. The points $(0, -11)$ and $(1, 33)$ are on the cubic $f'(x) = y$, which therefore has only one real intercept, between 0 and 1. This is on the same vertical line with the only maximum or minimum point of $f(x) = y$. Thus $f(x) = 0$ can have just two real roots. Now

$$f(0) = -41, \qquad f(\tfrac{1}{2}) = -42\tfrac{11}{16}, \qquad f(1) = -33.$$

Thus $(\frac{1}{2}, -43)$ is very close to the only minimum (or maximum) of $f(x) = y$. There are inflection points at $(-1, -23)$ and $(-2, -3)$. Clearly $f(x) = 0$ has just two real roots, one > 1 and one < -2.

A few more well-chosen points such as $(2, 49)$ and $(-3, 19)$ determine the curve. Thus the two real roots lie between 1 and 2 and between -3 and -2.

Exercise 17

1. Draw the graphs of $y = x$, $y = x^2$, $y = x^3$, and $y = x^4$ on the same set of axes.
2. Draw the graphs of

$$y = x^3 + 2x^2 + 3x - 5, \qquad y = x^3 + 2x^2 - 3x - 5.$$

3. Graph $y = x^3 - 3x^2 + 3$.
4. Graph $y = 3x^4 - 4x^3 - 6x^2 + 4$.
5. Graph $y = x^4 - 2x^3 - 12x^2 + 36x - 10$.
6. Can you assert that every cubic parabola has a maximum and a minimum point? an inflection point?

27. Behavior for x Large or Small

Theorem 31. Let $f(x)$ have leading coefficient 1, *and let h be the absolute value of the negative coefficient of largest absolute value. Then, for $a > h + 1$, $f(a) > 0$.*

Suppose that

$$f(x) = x^n + c_1x^{n-1} + c_2x^{n-2} + \cdots + c_n.$$

Let $d_i = -c_i$ if $c_i < 0$, $d_i = 0$ if $c_i \geqq 0$. Then for $a > 0$

$$f(a) \geqq a^n - d_1a^{n-1} - d_2a^{n-2} - \cdots - d_n.$$

If h is the largest of the d_i and if $a > 1$,

$$f(a) \geqq a^n - h(a^{n-1} + a^{n-2} + \cdots + 1)$$

$$\geqq a^n - h\frac{a^n - 1}{a - 1} > a^n - h\frac{a^n}{a - 1} = a^n\left(1 - \frac{h}{a - 1}\right).$$

Thus $f(a) > 0$ if

$$1 - \frac{h}{a - 1} > 0$$

that is, if $a > h + 1$.

Corollary 31. For x sufficiently large, $f(x)$ has the sign of its leading coefficient.

If every coefficient of $f(x)$ is positive, or if every coefficient is negative, the theorem is obvious. Otherwise choose $a > h + 1$ where h is the absolute value of the largest negative coefficient in

$$x^n + \frac{c_1}{c_0}x^{n-1} + \cdots + \frac{c_n}{c_0}.$$

Theorem 32. For x sufficiently small but positive, $f(x)$ has the sign of its term of lowest degree.

Let

$$f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_kx^{n-k} \qquad c_k \neq 0.$$

Then

$$\left(\frac{1}{a}\right) = \frac{c_0}{a^n} + \frac{c_1}{a^{n-1}} + \cdots + \frac{c_k}{a^{n-k}},$$

$$a^nf\left(\frac{1}{a}\right) = c_0 + c_1a + \cdots + c_ka^k.$$

Choose $a > 0$ so large that this expression has the sign of c_k. Then, for $x = 1/a$, x is positive and $f(x)$ has the sign of c_k.

28. Bounds

The theory of bounds as developed in § 12 holds for real roots as well as for rational roots. If we can find an upper bound for the zeros

of $f'(x)$ for which $f'(x)$ and $f(x)$ are positive, then this is an upper bound for the zeros of $f(x)$, for a curve which is positive and increasing is not approaching an intercept with the x axis. If we can find an upper bound for the zeros of $f''(x)$ for which $f''(x)$, $f'(x)$, and $f(x)$ are positive, this is an upper bound for $f(x)$, etc. Clearly that real root of $f(x) = 0$ which makes every derivative of $f(x)$ positive or 0 is the largest root of the equation. In other words, this is the best upper bound.

By Taylor's theorem,

$$f(x) = f(a) + f'(a)\cdot(x-a) + \frac{1}{2}f''(a)\cdot(x-a)^2 + \cdots + \frac{1}{n!}f^{(n)}(a)\cdot(x-a)^n.$$

We know that these coefficients are unique so that, if

$$f(x) = c_0(x-a)^n + c_1(x-a)^{n-1} + \cdots + c_{n-1}(x-a) + c_n,$$

then it necessarily follows that

$$c_{n-i} = \frac{1}{i!}f^{(i)}(a).$$

As we saw in § 16, c_n is the remainder obtained upon dividing $f(x)$ by $x - a$, c_{n-1} is the remainder obtained upon dividing the partial quotient by $x - a$, etc. We therefore have a quick method for determining these coefficients.

Example 1. Show that 2 is an upper bound for the roots of

$$f(x) = x^4 + 6x^3 + 12x^2 - 11x - 41 = 0.$$

We proceed as in § 16:

1	6	12	−11	−41	|	
	2	16	56	90	|	2
1	8	28	45	49		$= c_4$
	2	20	96			
1	10	48	141			$= c_3$
	2	24				
1	12	72				$= c_2$
	2					
1	14					$= c_1$

Hence

$$f(x) = (x-2)^4 + 14(x-2)^3 + 72(x-2)^2 + 141(x-2) + 49,$$

$$f(2) = 49, \quad f'(2) = 141, \quad f''(2) = 144, \quad f'''(2) = 84, \quad f^{\text{iv}}(2) = 24.$$

It is obvious that $f(x)$ can have no root > 2, since for such values $f(x) > 0$.

The graph of

$$y = g(x) = x^4 + 14x^3 + 72x^2 + 141x + 49$$

is identical with the graph of $f(x) = y$ except that the y axis is moved over two units. Since $f(x) = 0$ has a root between 1 and 2, and one between -2 and -3, $g(x) = 0$ has a root between -1 and 0 and a root between -4 and -5, and no other real root.

Example 2. Find an upper bound for the zeros of

$$f(x) = 3x^4 - x^3 + 5x^2 - 8x + 4.$$

We have

$$f'(x) = 12x^3 - 3x^2 + 10x - 8, \qquad f''(x) = 36x^2 - 6x + 10,$$

$$f'''(x) = 72x - 6.$$

Clearly $f'''(x) > 0$ for $x > \frac{1}{12}$, $f''(x) > 0$ for all x, $f'(x) > 0$ for $x > 1$. By substitution we find that $f(1) = 3$. Hence 1 is an upper bound.

Theorem 33. If a is an r-fold zero of $f(x)$, then for $\epsilon > 0$ sufficiently small

$$f(a-\epsilon), f'(a-\epsilon), \cdots, f^{(r)}(a-\epsilon)$$

alternate in sign, while

$$f(a+\epsilon), f'(a+\epsilon), \cdots, f^{(r)}(a+\epsilon)$$

are all of the same sign.

If a is an r-fold zero of $f(x)$, then

$$f(a) = f'(a) = \cdots = f^{(r-1)}(a) = 0, \qquad f^{(r)}(a) \neq 0.$$

By Taylor's theorem,

$$f(a+\epsilon) = \epsilon^r \left[\frac{1}{r!} f^{(r)}(a) + \cdots\right],$$

$$f'(a+\epsilon) = \epsilon^{r-1} \left[\frac{1}{(r-1)!} f^{(r)}(a) + \cdots\right],$$

. . . . . .

$$f^{(r)}(a+\epsilon) = f^{(r)}(a) + \cdots.$$

The term of lowest degree in ϵ in each case has the sign of $f^{(r)}(a)$, and so by Theorem 32 we may take ϵ so small that each function $f(a+\epsilon)$, $f'(a+\epsilon)$, $\cdots$, $f^{(r)}(a+\epsilon)$ has the sign of $f^{(r)}(a)$. Similarly

$$f(a-\epsilon) = \epsilon^r\left[\frac{(-1)^r}{r!}f^{(r)}(a)+\cdots\right],$$

$$f'(a-\epsilon) = \epsilon^{r-1}\left[\frac{(-1)^{r-1}}{(r-1)!}f^{(r)}(a)+\cdots\right],$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$f^{(r)}(a-\epsilon) = f^{(r)}(a)+\cdots.$$

Consequently we may take ϵ so small that these functions alternate in sign. Then, by taking ϵ the smallest of all these small numbers, we can make all $2r+2$ of these conditions hold simultaneously.

Theorem 34. If $f(x)$ is a polynomial of degree n, and if $q > p$, there are no more variations of sign in the sequence

$$f(q), f'(q), \cdots, f^{(n)}(q)$$

than there are in the sequence

$$f(p), f'(p), \cdots, f^{(n)}(p).$$

On the x axis lay off all the points where $f(x)$ is 0. Then lay off all the points where $f'(x)$ is 0. Then lay off all the points where $f''(x)$ is 0, and so forth. If $f(x)$ is of degree n, then $f^{(n)}(x)$ is a constant which is

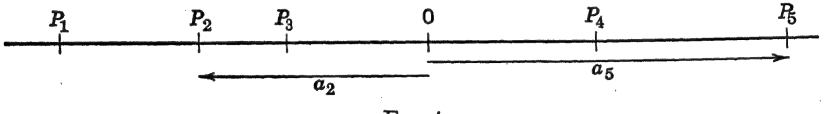

FIG. 4

not 0, namely the leading coefficient of $f(x)$ multiplied by $n!$. Thus $f^{(n)}(p) = f^{(n)}(q) \neq 0$. Now let $P_1, P_2, \cdots, P_k$ be the set of all of the points you have laid off on the x axis. Each of the functions $f(x)$, $f'(x)$, $\cdots$, $f^{(n)}(x)$ is a polynomial and hence can change sign only by crossing one of the points where it is zero. Hence as x moves from p to q the only places where the signs of these functions can possibly change are in crossing some point P_i.

Consider one of these points P_i and let a be its co-ordinate. Then either $f(a) = 0$ or, for some i, $f^{(i)}(a) = 0$ while $f^{(i-1)}(a) \neq 0$. But

$x = a$ may be a multiple root of $f^{(i)}(x) = 0$ of multiplicity r. Then we have

$$f^{(i)}(a) = f^{(i+1)}(a) = \cdots = f^{(i+r-1)}(a) = 0 \qquad r \geqq 1$$

while $f^{(i-1)}(a)$, if it exists, is not 0 and $f^{(i+r)}(a)$ is not 0. An application of Theorem 33 to the polynomial $f^{(i)}(x)$ shows that for ϵ sufficiently small the numbers

$$f^{(i)}(a + \epsilon), f^{(i+1)}(a + \epsilon), \cdots, f^{(i+r)}(a + \epsilon)$$

are all of the same sign, namely the sign of $f^{(i+r)}(a)$. Since this sequence of functions has no variations, it certainly has not gained any in passing over the point P_i. There may be other sequences of functions which vanish at $x = a$, but they too have gained no variation in passing over P_i. The other functions have not changed sign. Consequently the entire set of functions has no more variations at $x = a + \epsilon$ than at $x = a - \epsilon$ for ϵ sufficiently small. Since this is true for every point P_i, the theorem is proved.

Theorem 35. The Budan-Fourier Theorem. Let t be the number of zeros of $f(x)$ between $x = p$ and $x = q$ where $p < q$ and $f(p) \neq 0$ and $f(q) \neq 0$, an r-fold zero being counted as r zeros. Let V_q be the number of variations in sign in the sequence

$$f(q), f'(q), \cdots, f^{(n)}(q),$$

and let V_p be the number of variations in sign in the sequence

$$f(p), f'(p), \cdots, f^{(n)}(p).$$

Then $t = V_p - V_q - 2k$ where k is 0 or a positive integer.

Let a be an r-fold zero of $f(x)$ between p and q. That is,

$$f(a) = f'(a) = \cdots = f^{(r-1)}(a) = 0, \qquad f^{(r)}(a) \neq 0.$$

By Theorem 33, for ϵ sufficiently small

$$f(a - \epsilon), f'(a - \epsilon), \cdots, f^{(r-1)}(a - \epsilon), f^{(r)}(a)$$

alternate in sign, while

$$f(a + \epsilon), f'(a + \epsilon), \cdots, f^{(r-1)}(a + \epsilon), f^{(r)}(a)$$

are all of the same sign. Thus there is a loss of exactly r variations in sign in passing from $x = a - \epsilon$ to $x = a + \epsilon$. Hence, if t is the number of zeros of $f(x)$ between p and q, an r-fold zero being counted as r zeros, then

$$V_p - V_q \geqq t.$$

If b is a zero of one of the functions $f'(x), \cdots, f^{(n-1)}(x)$ but not a zero of $f(x)$, then $f(b-\epsilon)$ and $f(b+\epsilon)$ have the same sign, and $f^{(n)}(b)$ is a non-zero constant. Thus, in passing from $x = b - \epsilon$ to $x = b + \epsilon$, the functions lose an even number of variations, if any. Thus

$$V_p - V_q = t + 2k.$$

Consider the polynomial $f(x) = x^4 - 1$. Then $f'(x) = 4x^3$, $f''(x) = 12x^2$, $f'''(x) = 24x$, $f^{\text{iv}}(x) = 24$. For $\epsilon = 0.1$,

	$f(x)$	$f'(x)$	$f''(x)$	$f'''(x)$	$f^{\text{iv}}(x)$
$x = -0.1$	$-$	$-$	$+$	$-$	$+$
$x = 0$	$-$	0	0	0	$+$
$x = 0.1$	$-$	$+$	$+$	$+$	$+$

While $x = 0$ is not a root of $f(x) = 0$, it is a triple root of $f'(x) = 0$. Then

$$f'(0-\epsilon), f''(0-\epsilon), f'''(0-\epsilon), f^{\text{iv}}(0-\epsilon)$$

alternate in sign, while

$$f'(0+\epsilon), f''(0+\epsilon), f'''(0+\epsilon), f^{\text{iv}}(0+\epsilon)$$

all have the sign of $f^{\text{iv}}(0)$.

Corollary 35. Descartes' Rule of Signs. The number of positive roots of the equation

$$f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_n = 0 \qquad c_0 > 0$$

is equal to the number of variations in the signs of the coefficients, or this number decreased by an even integer.

Let $p = 0$, and let q be so large that $f(q), f'(q), \cdots, f^{(n)}(q)$ are all positive. The coefficients have the signs of $f(0), f'(0), \cdots, f^{(n)}(0)$ so that V_p is the number of variations in the signs of the coefficients and $V_q = 0$. Then the number of positive roots is $t = V_p - 2k$.

Exercise 18

1. Use Theorem 30 to obtain an upper bound for the roots of the equation

$$2x^6 + x^5 - 9x^4 - 6x^3 - 5x^2 - 7x + 6 = 0.$$

Can you obtain a better upper bound by other methods?

2. The polynomial

$$f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8$$

has a 3-fold zero at $x = 2$. Show that, for $x = 2.1$, $f(x)$, $f'(x)$, $f''(x)$, $f'''(x)$ all have the same sign, whereas, for $x = 1.9$, they alternate in sign.

3. By Descartes' rule of signs find the number of positive roots of

$$x^5 + x^4 - 2x^3 - x - 1 = 0.$$

4. Find the number of real roots of the equation

$$x^4 + x^2 - 3x - 1 = 0.$$

5. Find the number of real roots of the equation

$$x^4 + x^2 - 5 = 0.$$

6. By Descartes' rule of signs show that, for n even, a number $a > 0$ has two real nth roots, whereas, if n is odd and $a < 0$, there is just one real nth root.

7. Find the number of positive roots of the equation

$$x^5 + x^3 - 3x^2 + x - 3 = 0.$$

Hint. Multiply the left member by $x + 1$. Does this change the number of positive roots?

8. Find the number of positive roots of the equation

$$x^5 + 2x^3 - x^2 + x - 1 = 0.$$

9. By the Budan-Fourier theorem find the number of real roots of

$$x^3 - 3x + 1 = 0$$

that lie between 0 and 2.

10. Find the number of real roots of the equation

$$x^4 - 2x^3 + x^2 - x - 7 = 0$$

that lie between 1 and 5.

11. Find the number of real roots of

$$x^5 + x^4 - 7x^3 - 22x^2 + x + 1 = 0$$

that lie between -2 and 4. *Hint.* Break the interval $(-2, 4)$ into subintervals.

12. The equation

$$x^3 - 9x - 9 = 0$$

has a root between 3 and 4. Find another equation whose roots are those of the given equation each decreased by 3.

29. The Sturm Functions

Let $f(x)$ be a real polynomial, and denote it by $f_0(x)$. Denote $f'(x)$ by $f_1(x)$. Proceed as in the Euclid algorithm to find

$$\begin{aligned} f_0(x) &= q_1(x)\cdot f_1(x) - f_2(x), \\ f_1(x) &= q_2(x)\cdot f_2(x) - f_3(x), \\ f_2(x) &= q_3(x)\cdot f_3(x) - f_4(x), \\ &\cdots\cdots\cdots\cdots \\ f_{k-2}(x) &= q_{k-1}(x)\cdot f_{k-1}(x) - f_k \end{aligned}$$

where $f_i(x)$ is 0 or of degree less than the degree of $f_{i-1}(x)$ and f_k is a constant. The signs of the remainders are reversed from those in the usual Euclid process. At any stage $f_i(x)$ may be multiplied by a positive constant, but the sign must be carefully preserved.

Clearly the above Sturm process is a refinement of the greatest common divisor process of Euclid, so that the last non-vanishing remainder is a greatest common divisor of $f(x)$ and $f'(x)$.

Since f_k is a constant, it can be taken to be 0 or 1 or -1. If it is 0, $f_{k-1}(x)$ is a greatest common divisor of $f(x)$ and $f'(x)$ of degree greater than 0 so that $f(x)$ has at least one multiple zero. Then $f(x)/f_{k-1}(x)$ has only simple zeros. We shall assume from now on that $f(x)$ has only simple zeros.

Lemma 1. For no value $x = a$ can two consecutive functional values $f_i(a)$ and $f_{i+1}(a)$ be 0.

For, if $f_{i+1}(a) = f_i(a) = 0$, from the equations of the Sturm process we should have $f_{i-1}(a) = 0$, and from this it would follow that $f_{i-2}(a) = 0$, and so on, and finally that $f'(a) = f(a) = 0$. But this would imply that a was a multiple zero of $f(x)$, which we assumed not to exist.

Lemma 2. If $f_i(a) = 0$, then $f_{i-1}(a)$ and $f_{i+1}(a)$ have opposite signs.

For

$$f_{i-1}(a) = q_i(a)\cdot f_i(a) - f_{i+1}(a).$$

Lemma 3. If a is zero of $f_i(x)$ and $i > 0$, then for $\epsilon > 0$ sufficiently small the sequences

$$f_0(a-\epsilon), f_1(a-\epsilon), \cdots, f_k(a-\epsilon),$$

$$f_0(a+\epsilon), f_1(a+\epsilon), \cdots, f_k(a+\epsilon)$$

show the same number of variations in sign.

For, if ϵ is taken so small that $f_{i-1}(a-\epsilon)$ and $f_{i-1}(a+\epsilon)$ have the same sign, and $f_{i+1}(a-\epsilon)$ and $f_{i+1}(a+\epsilon)$ have the same sign, then

the sequence

$$f_{i-1}(a-\epsilon), f_i(a-\epsilon), f_{i+1}(a-\epsilon)$$

will exhibit one variation, as also will

$$f_{i-1}(a+\epsilon), f_i(a+\epsilon), f_{i+1}(a+\epsilon),$$

regardless of whether f_i changes sign or not.

Lemma 4. If $f(a) = 0$, then for $\epsilon > 0$ sufficiently small the sequence

$$f_0(a-\epsilon), f_1(a-\epsilon), \cdots, f_k(a-\epsilon)$$

exhibits exactly one more variation in sign than the sequence

$$f_0(a+\epsilon), f_1(a+\epsilon), \cdots, f_k(a+\epsilon).$$

Choose ϵ so small that $f'(x)$ has no zero in the interval $a-\epsilon$ to $a+\epsilon$, and that $f(a \pm \epsilon)$ and $f_1(a \pm \epsilon)$ have the same signs as their first coefficients:

$$f(a \pm \epsilon) = \pm \epsilon f_1(a) + \cdots,$$

$$f_1(a \pm \epsilon) = f_1(a) + \cdots.$$

Evidently $f(a-\epsilon)$ and $f_1(a-\epsilon)$ are of unlike signs while $f(a+\epsilon)$ and $f_1(a+\epsilon)$ are of like sign.

Theorem 36. The Sturm Theorem. Let $f(x)$ have simple zeros and let V_p be the number of variations in sign in the sequence of numbers

$$f(p), f_1(p), \cdots, f_k(p).$$

Then, if $p < q$, the number of real zeros of $f(x)$ between p and q is exactly $V_p - V_q$.

For, as x increases from p to q, one variation is subtracted for every zero of $f(x)$ which is passed over, and no variation is subtracted for any other change in sign of the functions.

Example. Use Sturm's theorem to isolate the real roots of

$$x^5 + 5x^4 - 20x^2 - 10x + 2 = 0.$$

We find the Sturm functions to be

$$f_0(x) = x^5 + 5x^4 - 20x^2 - 10x + 2, \qquad f_1(x) = x^4 + 4x^3 - 8x - 2,$$

$$f_2(x) = x^3 + 3x^2 - 1, \qquad f_3(x) = 3x^2 + 7x + 1, \qquad f_4(x) = 17x + 11,$$

$$f_5(x) = 1.$$

By setting $x = -\infty, 0, \infty$, we readily see that there are 3 negative roots and 2 positive roots. All roots are between -10 and 10, and in fact

between -5 and 5. We then have to try all integral values between -5 and 5. The work may be arranged as follows:

	$-\infty$	-10	-5	-4	-3	-2	-1	0	1	2	5	10	∞
f_0	$-$	$-$	$-$	$-$	$+$	$-$	$-$	$+$	$-$	$+$	$+$	$+$	$+$
f_1	$+$	$+$	$+$	$+$	$-$	$-$	$-$	$-$	$-$	$+$	$+$	$+$	$+$
f_2	$-$	$-$	$-$	$-$	$-$	$+$	$+$	$-$	$+$	$+$	$+$	$+$	$+$
f_3	$+$	$+$	$+$	$+$	$+$	$-$	$-$	$+$	$+$	$+$	$+$	$+$	$+$
f_4	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$+$	$+$	$+$	$+$	$+$	$+$
f_5	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$
var.	5	5	5	5	4	3	3	2	1	0	0	0	0

Thus there is a root between -4 and -3, a root between -3 and -2, a root between -1 and 0, a root between 0 and 1, and a root between 1 and 2.

Exercise 19

Find the Sturm functions and isolate the roots of

1. $x^3 - 2x - 2 = 0$,
2. $x^3 - 2x^2 - 2 = 0$,
3. $x^3 - 2x^2 - 5x + 7 = 0$,
4. $x^4 + 6x^3 + 12x^2 - 11x - 41 = 0$,
5. $x^4 + x^3 - 7x^2 - x + 5 = 0$.

6. Show that, for the cubic equation $x^3 + px + q = 0$, $p \neq 0$, the Sturm functions can be taken to be

$$f(x), f'(x), f_2(x) = -2px - 3q, \qquad f_3(x) = -4p^3 - 27q^2.$$

Thus show that the cubic has three real roots if and only if the discriminant $\Delta = -4p^3 - 27q^2$ is greater than 0.

7. Show that the cubic $x^3 + 1.0342x^2 - 6.3182x - 0.9928 = 0$ has a root between 2 and 3. [Change to a reduced cubic and apply Problem 6.]

30. Rule of False Position

The roots of an equation are said to be *isolated* when intervals have been determined each of which contains just one root. To be useful these intervals should be small, usually between consecutive integers, or, better, between consecutive tenths. A refinement is impossible until we have decided which root it is that we wish to approximate.

If (x_1, y_1) and (x_2, y_2) are two points on the curve $y = f(x)$, the equation of the line joining them is

$$y - y_1 = \frac{y_1 - y_2}{x_1 - x_2}(x - x_1)$$

and this secant line cuts the x axis at the point whose x co-ordinate is

$$x_0 = x_1 - y_1 \frac{x_1 - x_2}{y_1 - y_2}.$$

If y_1 and y_2 are of opposite sign so that $f(x)$ has a zero between x_1 and x_2, then x_0 is nearer to this zero than is either x_1 or x_2. By the sign of y_0 we can determine in which of the intervals x_1 to x_0 or x_0 to x_2 the zero lies, whereupon the process can be repeated.

The process we have just outlined is known as the rule of false position, and has the advantage of always giving a better value than either of those with which we began. It can be used to refine the solution to as many decimal places as we please, but it can become very tedious. When we are close to a root, other methods are much more rapid.

Example. Find a second approximation to the root of

$$x^4 + 6x^3 + 12x^2 - 11x - 41 = 0$$

which lies between -3 and -2.

We now enlarge our scale. In the larger scale the curve has become more nearly straight. We shall use the rule of false position but avoid

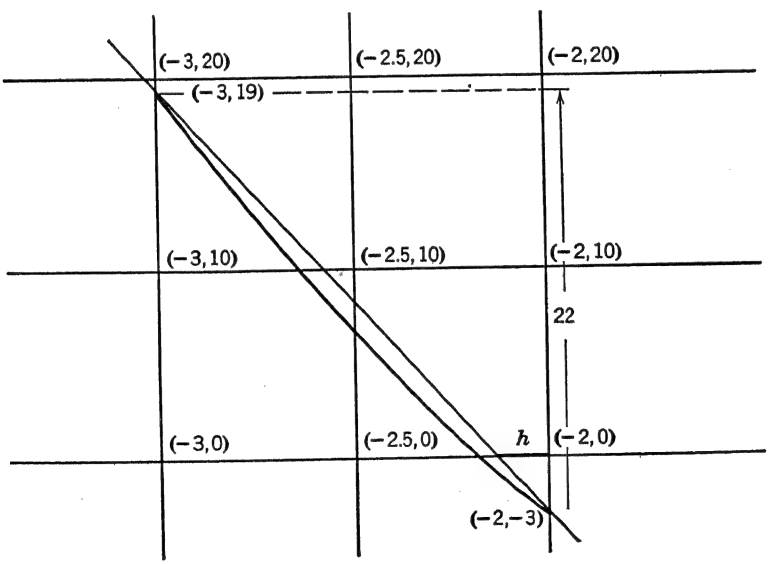

FIG. 5

the formula. If the curve were straight, the crossing point could be determined by similar triangles. Thus, denoting the (positive) distance of this point from the point $(-2, 0)$ by h, we have

$$h/3 = 1/22, \qquad h = 0.14.$$

Hence the crossing point of the secant would be at $x = -2.14$.

But it must be remembered that the curve is concave upward in this interval so that we must try values to the left of the value which we have obtained. We find

$$f(-2.2) = -1.6024, \qquad f(-2.3) = 2.7621.$$

Hence -2.2 is the second approximation.

After the second approximation is obtained, there are more rapid methods for obtaining further refinements.

Exercise 20

Find intervals of length 0.1 in which each of the roots of the following equations lie:

1. $x^3 - 2x - 2 = 0$,
2. $x^3 - 2x^2 - 2 = 0$,
3. $x^3 - 2x^2 - 5x + 7 = 0$,
4. $x^4 + x^3 - 7x^2 - x + 5 = 0$.
5. $x^5 - 31 = 0$.

31. Newton's Method

This method of approximation is based upon the principle of using the tangent to the curve instead of the secant, and thus the knowledge of only one point near the zero of the polynomial is required. Let this nearby point be denoted by (x_1, y_1). The equation of the tangent to $y = f(x)$ at this point is

$$y - y_1 = f'(x_1) \cdot (x - x_1)$$

and the tangent intersects the x axis at the point whose x co-ordinate is

$$x_0 = x_1 - y_1/f'(x_1) = x_1 - f(x_1)/f'(x_1).$$

Let us continue with the example of the last section. We had obtained $(x_1, y_1) = (-2.2, -1.6024)$ so that the next approximation is

$$x = -2.2 + 1.6024/-19.272 = -2.283$$

which is for most purposes a sufficiently good approximation to the root. The process may be repeated if further accuracy is desired.

It is impossible to state in general how many decimal places to keep, for this differs from equation to equation. Usually each repetition of

the Newton process just about doubles the number of significant figures in the approximation. The last digit may not be correct, but it may be better to keep it than to replace it with a 0. Thus, if the correct value to three places of the root is -2.284, our result -2.283 is closer than -2.28.

Exercise 21

By Newton's method find to four decimal places the real root of

1. $x^3 - 2x - 2 = 0$, 2. $x^3 - 2x^2 - 2 = 0$.

3. Find to five places the largest root of

$$x^3 - 2x^2 - 5x + 7 = 0.$$

4. Find to four places the roots of

$$x^4 + x^3 - 7x^2 - x + 5 = 0$$

which lie between -4 and -3, and between 0 and 1.

5. Find the fifth root of 31 to five places.

6. Why is Newton's method unsatisfactory for finding a root which is multiple?

32. Horner's Method

While the Horner method is essentially equivalent to the Newton method in that the approximation is made by means of the tangent, it makes use of computational methods which are applicable only to polynomials. If a is known to be close to a zero of $f(x)$, we may write

$$f(x) = c_0(x - a)^n + c_1(x - a)^{n-1} + \cdots + c_{n-1}(x - a) + c_n.$$

Since $x - a$ is small, its powers are still smaller, and, if x is a zero of $f(x)$ so that $f(x) = 0$, then it is approximately true that

$$c_{n-1}(x - a) + c_n = 0.$$

That is,

$$x = a - c_n/c_{n-1}.$$

Of course $c_n = f(a)$ and $c_{n-1} = f'(a)$ so that $y = c_{n-1}(x - a) + c_n$ is the tangent to $y = f(x)$ at the point where $x = a$, and we see that the method is equivalent to that of Newton.

But Horner's arrangement of the calculation is elegant, as we shall illustrate.

Example. Find to four decimal places the root of the equation

$$f(x) = x^3 + 1.0342x^2 - 6.3182x - 0.9928 = 0$$

which lies between 2 and 3.

We find that

$$f(2) = -1.4924, \qquad f(3) = 16.3604$$

so that by the rule of false position the root is about 2.08. We shall use the nearest tenth, namely 2.1, and decrease the roots of $f(x) = 0$ by 2.1. (See § 16.)

1	1.0342	−6.3182	−0.9928	
	2.1	6.58182	0.553602	2.1
1	3.1342	0.26362	−0.439198	
	2.1	10.99182		
1	5.2342	11.25544		
	2.1			
1	7.3342			

The root of

$$f_1(x) = x^3 + 7.3342x^2 + 11.25544x - 0.439198 = 0$$

is so close to 0 (<0.1) that we obtain an approximation to it by solving the linear equation

$$11.25544h - 0.439198 = 0.$$

This gives $h = 0.039021$, but we are justified in retaining 0.038 or 0.039 at best.

Let us now decrease the roots of $f_1(x) = 0$ by 0.038:

1	7.3342	11.25544	−0.439198	
	0.038	0.2801436	0.4383521768	0.038
1	7.3722	11.5355836	−0.0008458232	
	0.038	0.2815876		
1	7.4102	11.8171712		
	0.038			
1	7.4482			

The root of

$$x^3 + 7.4482x^2 + 11.8171712x - 0.0008458232 = 0$$

is very close to 0 so that the approximation

$$h = 0.0008458232/11.8171712 = 0.000071576$$

is close. Presumably the physical data which gave rise to the given equation is meaningful only to four decimal places so that anything more than four-place accuracy in the root is wasted effort. This approximation is $x = 2.1380$, for

$$f(2.1380) = -0.0008458232, \qquad f(2.1381) = 0.000335968403.$$

In Horner's method it is customary to keep the approximation below the true value, but this is by no means necessary. If a value too large has been used, the next approximation will turn out to be negative. In fact, the effect of a poor appproximation is merely to slow up the process and presumably to necessitate another step, but it will not invalidate the final result unless an actual error of computation has been made.

Exercise 22

By Horner's method find to four decimal places the roots of

1. $x^3 - 2x - 2 = 0$,
2. $x^3 - 2x^2 - 5 = 0$ between 2 and 3.
3. Find to five places the positive root of

$$x^4 - 2x^3 + x^2 - 3 = 0.$$

4. Find to four places the roots of

$$x^4 + x^3 - 7x^2 - x + 5 = 0$$

which lie between -1 and 0, and between 2 and 3.

5. Find the length of the longest strip of carpet 3 feet wide that can be laid in a room 20 feet by 30 feet.

CHAPTER

5

Complex Roots

33. The Complex Numbers

The positive real numbers are useful in measuring magnitudes which have the single property of size. The positive and negative real numbers have the properties of size and direction to the right or left on a horizontal line. They are completely representable by the distances of the points of an unlimited straight line, such as the x axis, from a fixed point called the origin.

The reader doubtless already is aware of magnitudes, such as forces and velocities, which have the attributes of direction in a plane as well

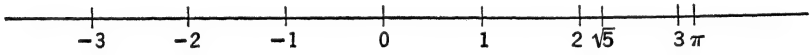

FIG. 6

as size. These magnitudes can be represented by vectors, each determined by its length and its direction. This fact raises the question whether such magnitudes can be represented by a new kind of number, and, if so, how these numbers behave. If we confine our attention to vectors which lie in the same plane, we shall discover a new number system, the field of *complex numbers*, which is even more remarkable than the real field.

If a real number a is multiplied by -1, its vector may be thought of as being subjected to a rotation about the origin through a positive angle of 180°. To introduce our new numbers, we shall define a number i whose effect as a multiplier is to rotate the vector a through a positive angle of 90°. Then $i \cdot 1 = i$ corresponds to the vector which is of length 1 extending upward from the origin perpendicular to the axis of reals. Since two applications of i as a multiplier have the effect of multiplying by -1, it is clear that we must define $i^2 = -1$.

If a is any positive number, ia is a vector extending upward from the origin 0 of length a. Similarly the number $-5i$ is obtained by rotating

the vector -5 through 90° in a positive direction. Hence the vector corresponding to $-5i$ extends downward from 0 a distance of 5 units. The number bi where b is real is called a *purely imaginary number*.

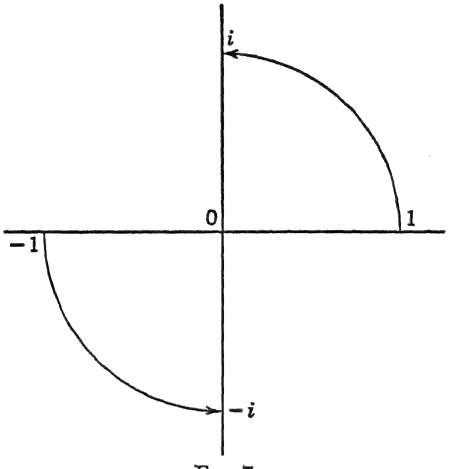

Fig. 7

In defining the sum $a + bi$ of a real and a purely imaginary number we shall take our cue from the composition of forces. The sum or resultant of two forces is known to be representable by the vector which is the diagonal of the parallelogram whose sides are the component

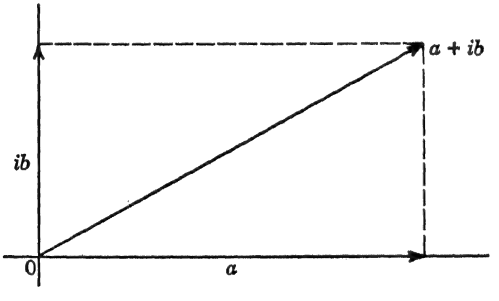

Fig. 8

forces. Hence we shall define $a + bi$ as the number whose vector has the component a along the axis of reals and the component b along the axis of imaginaries.

Let $a + bi$ and $c + di$ be two complex numbers. The real component of their sum or resultant is $a + c$, and the imaginary component has

the length $b + d$ along the imaginary axis. Thus we define

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

Since the triangles OAM and CPN are congruent, $OM = a$, $OR = c$,

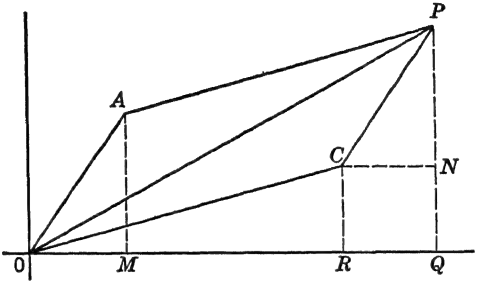

FIG. 9

and it is clear that $OQ = a + c$ and $QP = b + d$. Thus the diagonal OP actually corresponds to the number

$$(a + c) + (b + d)i.$$

34. Absolute Value and Argument

The length of a vector $a + bi$ is called its *absolute value*. This is equal to $\sqrt{a^2 + b^2}$. The reflection of $a + bi$ on the x axis, namely the vector $a - bi$, is called the *conjugate* of $a + bi$. The product of a vector and its conjugate is called the *norm* of each. It is the square of the absolute value.

We shall call the angle which the vector $a + bi \neq 0$ makes with the positive direction of the real axis its *argument*. This is unique only if we take it between 0° and 360°, the latter excluded. Thus the absolute value r and the argument θ are merely the polar co-ordinates of the point whose Cartesian co-ordinates are (a, b). Thus

$$a = r \cos \theta, \qquad b = r \sin \theta$$

so that

$$a + bi = r(\cos \theta + i \sin \theta).$$

The number i was defined so that, for every real number b, bi is the vector of the same absolute value $|b|$ and with its argument increased by 90°. In fact, if we define multiplication by i to be distributive, namely

$$i(a + bi) = ia + i^2 b = -b + ai,$$

it is clear that every vector, $a + bi$, is merely rotated through 90° upon multiplication by i.

Even more generally, we may define the multiplication of two com-

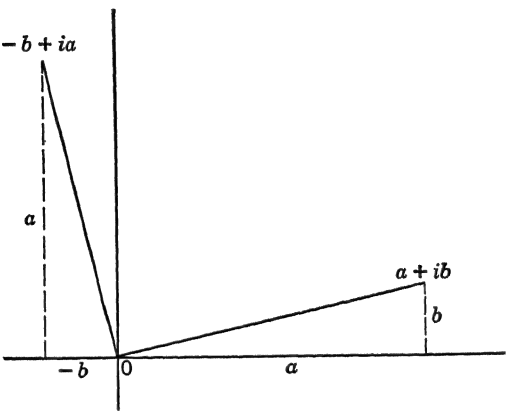

FIG. 10

plex numbers by the distributive law:

$$(a + bi)(c + di) = ac - bd + (ad + bc)i.$$

If

$$a + bi = r(\cos\theta + i\sin\theta), \qquad c + di = s(\cos\phi + i\sin\phi),$$

then

$$\begin{aligned}(a + bi)(c + di) &= rs[(\cos\theta\cos\phi - \sin\theta\sin\phi) \\ &\quad + i(\cos\theta\sin\phi + \sin\theta\cos\phi] \\ &= rs[\cos(\theta + \phi) + i\sin(\theta + \phi)].\end{aligned}$$

Therefore in multiplying any vector

$$c + di = s(\cos\phi + i\sin\phi)$$

by another vector

$$a + bi = r(\cos\theta + i\sin\theta),$$

the multiplicand is rotated through the amplitude of the multiplier, and its length is multiplied by the absolute value of the multiplier.

Since $i^2 = -1$, it is clear that, for every positive number a, $(i\sqrt{a})^2 = -a$. But it is also true that $(-i\sqrt{a})^2 = -a$. It will be necessary, then, to define the symbol $\sqrt{-a}$ when the radicand is negative. We define it to be the principal value, namely

$$\sqrt{-a} = i\sqrt{a}.$$

The existence of the two square roots of a negative number makes it necessary to watch the use of radicals carefully. If a and b are positive, we are familiar with the identity

$$\sqrt{a}\cdot\sqrt{b} = \sqrt{ab},$$

and may be slightly surprised that it fails to hold when a and b are negative. But this is the case. Thus

$$\sqrt{-5}\cdot\sqrt{-3} = i\sqrt{5}\cdot i\sqrt{3} = -\sqrt{15}.$$

Example. Write $\dfrac{3+\sqrt{-5}}{2+\sqrt{-3}}$ in the form $a + bi$.

The fraction is equal to $\dfrac{3+i\sqrt{5}}{2+i\sqrt{3}}$. If we multiply both numerator and denominator by the conjugate of the denominator, we obtain

$$\frac{(3+i\sqrt{5})(2-i\sqrt{3})}{(2+i\sqrt{3})(2-i\sqrt{3})} = \frac{6+\sqrt{15}+i(2\sqrt{5}-3\sqrt{3})}{7}.$$

The denominator, being the norm of $2 + i\sqrt{3}$, is a real number. Hence

$$a = \frac{6+\sqrt{15}}{7}, \qquad b = \frac{2\sqrt{5}-3\sqrt{3}}{7}$$

Exercise 23

1. Write in the form $a + bi$:

   (*a*) $3 - \sqrt{-4}$, (*b*) $2 + \sqrt{-5}$, (*c*) $1 - \sqrt{-27/4}$.

2. Write in the form $a + bi$:

   (*a*) $\dfrac{2-i}{1+2i}$, (*b*) $\dfrac{2}{i-1} + \dfrac{2}{i+1}$, (*c*) $\dfrac{5+\sqrt{-3}}{2-2\sqrt{-3}}$.

3. Prove that $a + bi = 0$ if and only if its absolute value is 0.
4. Write $(-\frac{1}{2} - i\frac{1}{2}\sqrt{3})^3$ in the form $a + bi$.
5. Show that $-\frac{1}{2} + i\frac{1}{2}\sqrt{31}$ is a solution of the equation

$$x^2 + x + 8 = 0.$$

6. Find the absolute value and the argument of

   (*a*) $\dfrac{-1-i\sqrt{3}}{2}$, (*b*) $\dfrac{1-i\sqrt{3}}{2}$.

7. Prove that the complex numbers form a field.

35. Powers and Roots

Theorem 37. DeMoivre's Theorem. If

$$\alpha = r(\cos\phi + i\sin\phi)$$

is any complex number, then for every positive integer n

$$\alpha^n = r^n(\cos n\phi + i\sin n\phi).$$

The proof is by induction. The theorem is trivially true for $n = 1$. The induction hypothesis is

$$\alpha^{n-1} = r^{n-1}[\cos(n-1)\phi + i\sin(n-1)\phi].$$

If we multiply each side by α, and remember that in multiplying a number by $r(\cos\phi + i\sin\phi)$ we multiply its absolute value by r and add ϕ to its argument, we have the proof. For, by taking $n = 2$, we show that the theorem is true for $n = 2$. Then, by taking $n = 3$, we show that the theorem is true for $n = 3$, and so on for every n.

More generally, if k is any rational integer and

$$\alpha = r\left[\cos\left(\frac{\phi}{n} + \frac{2k\pi}{n}\right) + i\sin\left(\frac{\phi}{n} + \frac{2k\pi}{n}\right)\right],$$

then α^n is independent of k. For by DeMoivre's theorem

$$\begin{aligned}\alpha^n &= r^n[\cos(\phi + 2k\pi) + i\sin(\phi + 2k\pi)] \\ &= r^n(\cos\phi + i\sin\phi).\end{aligned}$$

This might seem to indicate that there are infinitely many numbers having the same nth power. Actually, however, just n of them are distinct. If we let $k = 0, 1, \cdots, n-1$, we get distinct values of α, but $k = n$ gives the same value as $k = 0$, etc.

Theorem 38. If α is a complex number not 0, the equation $x^n = \alpha$ has just n distinct complex solutions.

If $\alpha = r(\cos\phi + i\sin\phi)$, these solutions are

$$\sqrt[n]{r}\left[\cos\left(\frac{\phi}{n} + \frac{2k\pi}{n}\right) + i\sin\left(\frac{\phi}{n} + \frac{2k\pi}{n}\right)\right] \quad k = 0, 1, \cdots, n-1$$

where $\sqrt[n]{r}$ is the unique positive nth root of the positive number r. These n nth roots of α are represented by vectors which are the equally

spaced spokes of a wheel of radius $\sqrt[n]{r}$. Since an equation such as $x^n - \alpha = 0$ cannot have more than n distinct solutions (Theorem 25), we have obviously solved it completely.

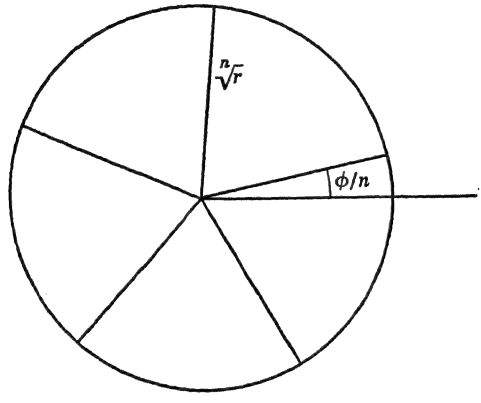

FIG. 11

36. Quadratic and Cubic Polynomials

As we saw in § 2, the quadratic function can be factored

$$x^2 + bx + c = \left(x - \frac{-b + \sqrt{b^2 - 4c}}{2}\right)\left(x - \frac{-b - \sqrt{b^2 - 4c}}{2}\right).$$

Hence the equation $x^2 + bx + c = 0$ has the two roots

$$x_1 = \frac{-b + \sqrt{b^2 - 4c}}{2}, \qquad x_2 = \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

Suppose that a, b, and c are real. If $b^2 - 4c$ is positive, the roots are real and distinct. If $b^2 - 4c = 0$, the roots are real and equal. If $b^2 - 4c < 0$, the roots are distinct and not real.

A cubic equation such as

$$x^3 + c_1x^2 + c_2x + c_3 = 0$$

has a real root, since it is of odd degree (§ 25, Problem 6). Let this root be a. Then by the factor theorem (Corollary 24)

$$x^3 + c_1x^2 + c_2x + c_3 = (x - a)(x^2 + bx + c)$$

so that every cubic polynomial with real coefficients can be factored into a linear and a quadratic polynomial, both with real coefficients.

If a cubic equation with real coefficients has three real roots, it can be solved by the use of trigonometric functions. We may assume that the equation has been replaced by a reduced cubic (§ 17) of the form

$$y^3 + py + q = 0,$$

for the roots of the given cubic are readily obtained from the roots of this reduced cubic. Since the three roots are real, we know (§ 29, Problem 6) that

$$\Delta = -4p^3 - 27q^2 > 0, \qquad p < 0.$$

Let us write $y = kz$, $k \neq 0$, so that the equation becomes

$$z^3 + \frac{pz}{k^2} + \frac{q}{k^3} = 0.$$

We may identify this equation with the trigonometric identity

$$\cos^3 A - \tfrac{3}{4}\cos A - \tfrac{1}{4}\cos 3A = 0$$

by taking

$$\cos A = z, \qquad p/k^2 = -3/4, \qquad \cos 3A = -4q/k^3.$$

The second equation tells us that we must take

$$k = \sqrt{-4p/3}.$$

Since $p < 0$, k is real and we select the positive value. Then

$$-4p^3 - 27q^2 > 0, \qquad 0 < \frac{27q^2}{-4p^3} < 1,$$

$$\cos 3A = \frac{-4q}{k^3} = \pm\sqrt{\frac{27q^2}{-4p^3}},$$

so that $\cos 3A$ lies between -1 and 1, and there is a real angle $3A$ between $0°$ and $180°$ whose cosine is $-4q/k^3$. Then for A we have the three values

$$A_1 = 3A/3, \qquad A_2 = A_1 + 120°, \qquad A_3 = A_1 + 240°.$$

Then the reduced cubic has the three real roots

$$y_1 = k\cos A_1, \qquad y_2 = k\cos A_2, \qquad y_3 = k\cos A_3.$$

Example. Find the real roots of

$$x^3 + 1.0342x^2 - 6.3182x - 0.9928 = 0.$$

Set $x = y - 0.3447$. The reduced cubic is

$$y^3 - 6.6747 + 1.2669 = 0.$$

Since the discriminant is $\Delta = 1146.2$, all three roots are real.

$p = -6.6747$, $q = 1.2669$, $\cos 3A < 0$.

$\log \lvert p \rvert$	$= 0.82443$	$\log q$	$= 0.10275$
$\log \frac{4}{3}$	$= 0.12494$	$\log 4$	$= 0.60206$
$\log k^2$	$= 0.94937$	$\log 4q$	$= 0.70481$
$\log k$	$= 0.47468$	$\log k^3$	$= 1.42404$
$\log k^3$	$= 1.42404$	$\log 4q/k^3$	$= 9.28077 - 10$
			$78° 59' 45''$
			$3A = 101° 0' 15''$

$A_1 = 33° 40' 5''$		$A_2 = 153° 40' 5''$		$A_3 = 273° 40' 5''$	
$\cos A_1 > 0$		$\cos A_2 < 0$		$\cos A_3 > 0$	
$\log \cos A_1$	$= 9.92026$	$\log \lvert \cos A_2 \rvert$	$= 9.95242$	$\log \cos A_3$	$= 8.80585$
$\log k$	$= 0.47468$		0.47468		0.47468
$\log y_1$	$= 0.39494$	$\log \lvert y_2 \rvert$	$= 0.42710$	$\log y_3$	$= 9.28069$
y_1	$= 2.4828$	y_2	$= -2.6736$	y_3	$= 0.19085$
	-0.3447		-0.3447		-0.3447
x_1	$= 2.1381$	x_2	$= -3.0183$	x_3	$= 0.15385$

Exercise 24

1. By DeMoivre's theorem find the cube roots of 1.
2. Find the fifth roots of 1.
3. Find the solutions of $x^3 + 5 = 0$.
4. Solve the equation $x^3 - 2 + 3i = 0$.
5. Find the discriminant of $y^3 - 12y + 12 = 0$, and solve.
6. Solve $y^3 - 3y + 1 = 0$.
7. Solve $y^3 - 30y - 20 = 0$.
8. Find the real solutions of $x^3 + 3x^2 - 3x - 9 = 0$.
9. Solve $x^3 + 6x^2 + 6x - 2 = 0$.
10. Solve $x^3 + 6x^2 + 8x - 1 = 0$.
11. A parallelepiped with square base has a volume of 28.31 cubic inches, and the altitude exceeds the length of the edge of the base by 5.92 inches. Find the length of the edge of the base.

37. The Fourth- and Fifth-Degree Polynomials

Theorem 39. Every quartic polynomial with real coefficients can be written as the product of two quadratic polynomials with real coefficients.

It is no essential restriction to assume that the polynomial is of the form

$$f(x) = x^4 + c_2x^2 + c_3x + c_4,$$

for every quartic polynomial can be written in this form after a linear transformation of the variable. Let us assume that

$$f(x) = (x^2 + kx + p)(x^2 + lx + q)$$

where k, p, l, and q are to be determined. If we multiply these factors together and equate coefficients, we obtain the conditions

$$k + l = 0, \quad p + q + kl = c_2, \quad lp + kq = c_3, \quad pq = c_4.$$

From these we immediately obtain

$$l = -k, \quad p + q - k^2 = c_2, \quad -kp + kq = c_3, \quad pq = c_4.$$

The second and third equations give

$$2kp = k^3 + kc_2 - c_3, \qquad 2kq = k^3 + kc_2 + c_3.$$

From the fourth equation we now have

$$4k^2c_4 = 4k^2pq = (k^3 + kc_2)^2 - c_3{}^2$$

so that k satisfies the equation

$$k^6 + 2c_2k^4 + (c_2{}^2 - 4c_4)k^2 - c_3{}^2 = 0.$$

This may be considered as a cubic equation in k^2, and therefore at least one value of k^2 is real. In fact, if $c_3 \neq 0$, by Descartes' rule of signs, at least one value of k^2 is positive, and, if $c_3 = 0$, one value of k^2 is 0. In any case, then, there is at least one value of k which is real. If $k \neq 0$, real values for p and q and l are obtainable from the relations

$$p + q = c_2 + k^2, \qquad p - q = -c_3/k \qquad l = -k.$$

If one value of k is 0, then $c_3 = 0$ and

$$f(x) = x^4 + c_2x^2 + c_4.$$

If $c_2{}^2 - 4c_4 \geqq 0$, this can be factored into real factors by the quadratic formula. If $c_2{}^2 - 4c_4 < 0$, then the equation defining k becomes

$$k^4 + 2c_2k^2 + (c_2{}^2 - 4c_4) = 0$$

which, by Descartes' rule of signs, has a positive root k^2, and a real non-zero value for k.

Once the quartic polynomial has been factored into quadratic factors, its zeros are obtainable by the quadratic formula.

Let us now consider the quintic polynomial

$$x^5 + c_1x^4 + c_2x^3 + c_3x^2 + c_4x + c_5.$$

Since it is of odd degree, it has a real factor $x - a$, and the quotient upon dividing the quintic by this linear factor is a polynomial of degree 4 with real coefficients. This, as we have just seen, can be written as a product of two real quadratic factors. It is therefore true that *every polynomial equation $f(x) = 0$ with real coefficients of degree $\leqq 5$ has as many complex roots, real or not real, as its degree.*

This is a special case of a very important theorem, first stated by D'Alembert in 1746 but not rigorously proved until about 1800, which is sometimes called the fundamental theorem of algebra. This theorem states that every polynomial equation of degree n with complex coefficients has a complex root (which may of course be real). It readily follows by a repeated application of this theorem that every equation with complex coefficients has exactly as many complex roots as its degree, an r-fold root counting as r roots. The proof of this theorem is not elementary, and is usually first made in a class in modern higher algebra or theory of functions of a complex variable.

It cannot be emphasized too strongly that the fundamental theorem proves the existence of roots but does not afford a good method for finding them. Even in the case of the real quintic, the real root whose existence we established so blithely can be effectively obtained in most instances only by an approximate method such as Horner's method.

Exercise 25

1. Factor $x^4 + 4x - 1$ into real quadratic factors.

2. Factor $x^4 + 4x^2 + x + 6$.

3. Factor $x^4 + 5x^2 + 2x + 8$.

4. Factor $x^4 + 4x^3 - 24x - 24$ into quadratic factors whose coefficients are real decimal numbers correct to four places.

5. Find the roots of $x^4 - 8x + 12 = 0$ in the form $a + bi$ where a and b are four-place decimals.

6. Show that, whether $k = 0$ or not, p and q are the roots of the quadratic $x^2 - (c_2 + k^2)x + c_4 = 0$. When does this give real values?

7. Solve $x^4 + 8x^3 + 42x^2 - 8x + 281 = 0$.

38. Conjugates

If $\alpha = a + ib$, the number $\bar{\alpha}$ obtained from α by replacing i by $-i$ is called the *conjugate* of α. Note that $\alpha = \bar{\alpha}$ if and only if α is real.

Theorem 40. The conjugate of the sum of two complex numbers is equal to the sum of the conjugates of the numbers. The conjugate of the product of two complex numbers is equal to the product of the conjugates of the factors.

Thus, if $\alpha = a + ib$ and $\beta = c + id$, then

$$\alpha + \beta = a + c + i(b + d),$$

$$\bar{\alpha} + \bar{\beta} = a - ib + c - id = a + c - i(c + d) = \overline{\alpha + \beta}$$

Also

$$\alpha\beta = ac - bd + i(ad + bc),$$

$$\bar{\alpha}\bar{\beta} = (a - ib)(c - id) = ac - bd - i(ad + bc) = \overline{\alpha\beta}.$$

A correspondence such as α corresponding to $\bar{\alpha}$ (written $\alpha \leftrightarrow \bar{\alpha}$) which is preserved under both addition and multiplication is called an *automorphism*. The field of real numbers has no automorphism except the trivial one by which every number corresponds to itself, and the complex field has none except the trivial one and the relation of conjugation. The graduate student in mathematics will encounter this concept repeatedly.

Theorem 41. If $f(x)$ has real coefficients and if α is a complex number, then $\overline{f(\alpha)} = f(\bar{\alpha})$.

Let

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

where the a's are real so that $\overline{a_i} = a_i$. Then

$$f(\alpha) = a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n.$$

Then by Theorem 40

$$\begin{aligned}\overline{f(\alpha)} &= \overline{a_0\alpha^n} + \overline{a_1\alpha^{n-1}} + \cdots + \overline{a_{n-1}\alpha} + \overline{a_n} \\ &= a_0\overline{\alpha^n} + a_1\overline{\alpha^{n-1}} + \cdots + a_{n-1}\bar{\alpha} + a_n \\ &= a_0\bar{\alpha}^n + a_1\bar{\alpha}^{n-1} + \cdots + a_{n-1}\bar{\alpha} + a_n = f(\bar{\alpha}).\end{aligned}$$

Theorem 42. Let $f(x)$ be a polynomial with complex coefficients, and let $\bar{f}(x)$ be the same polynomial with each coefficient replaced by its conjugate. Then $f(x)\cdot\bar{f}(x)$ is a polynomial with real coefficients.

If

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n,$$

the coefficient of x^{2n-i} in $f(x)\cdot\bar{f}(x)$ is

$$a_0\bar{a}_i + a_1\bar{a}_{i-1} + a_2\bar{a}_{i-2} + \cdots + a_{i-1}\bar{a}_1 + a_i\bar{a}_0 \quad a_j = 0 \text{ for } j > n.$$

Since this is equal to its own conjugate, it is real.

Theorem 43. If $f(x) = 0$ has real coefficients and has α as a root, then $\bar{\alpha}$ is also a root.

For, if $f(\alpha) = 0$, then $\overline{f(\alpha)} = \overline{0} = 0$, so that $\overline{f(\alpha)} = f(\bar{\alpha}) = 0$. Since $\alpha = \bar{\alpha}$ only if α is real, we have

Theorem 44. The non-real roots of an equation with real coefficients occur in conjugate pairs.

Let $\alpha = a + ib$. Then

$$\begin{aligned}(x - \alpha)(x - \bar{\alpha}) &= (x - a - ib)(x - a + ib)\\ &= (x - a)^2 + b^2 = x^2 - 2ax + a^2 + b^2.\end{aligned}$$

These coefficients are real. Hence if a polynomial $f(x)$ of degree n has a non-real root, $f(x)$ can be written as the product of a real quadratic factor and another factor with real coefficients of degree $n - 2$. A continuation of this argument proves

Theorem 45. Every polynomial with real coefficients can be written as a product of polynomials with real coefficients, each of degree 1 or of degree 2.

Exercise 26

1. Show that $|\alpha\beta| = |\alpha|\cdot|\beta|$.
2. Let $\alpha = r(\cos\theta + i\sin\theta)$, $\beta = s(\cos\phi + i\sin\phi)$. Show that

$$|\alpha + \beta|^2 = r^2 + s^2 + 2rs\cos(\theta - \phi).$$

3. Prove that $|\alpha + \beta| \leqq |\alpha| + |\beta|$. Illustrate geometrically. Why is this inequality called the "triangle property" of absolute value?
4. Let

$$\alpha = \pm\left(\sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} \pm i\sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}}\right)$$

where the second $\pm$ sign is the same as the sign of b. Find α^2.

5. Solve the quadratic equation $x^2 + x + 5ix + 5i - 12 = 0$. [First calculate its discriminant; then use Problem 4.]

6. Solve $x^2 + 0.2181x + 1.3425ix - 0.7932 + 0.6844i = 0$, obtaining the answer in the form $A + iB$ where A and B are four-place decimals.

CHAPTER 6

Relations among the Roots

39. Symmetric Functions

A polynomial such as

$$f(x, y, z) = x^2 + y^2 + z^2 - 13xyz$$

is said to be *symmetric* in the three letters x, y, and z if the function remains the same when any two of the letters are interchanged. The rational function

$$\frac{(a-b)^2(b-c)^2(c-a)^2}{a+b+c}$$

is symmetric in a, b, and c, while $(a-b)(b-c)(c-a)$ is not.

It is obvious that in a symmetric function such as

$$x^3 + y^3 + z^3 - xy - yz - zx$$

which is composed of parts of different degrees, each homogeneous part must itself be a symmetric function, since no term can go into a term of different degree under an interchange of letters. Thus both $x^3 + y^3 + z^3$ and $xy + yz + zx$ are symmetric functions.

Let $x_1, x_2, \cdots, x_n$ be n different indeterminates. If $x_1^3x_2^2x_3$, for instance, is any term in these indeterminates, then

$$\Sigma x_1^3x_2^2x_3$$

denotes the sum of all the different terms obtainable from $x_1^3x_2^2x_3$ by permuting the subscripts 1, 2, $\cdots$, n in all possible ways. Such a function is obviously symmetric and is called a *sigma function.*

The particular sigma functions

$$\begin{aligned}
\Sigma x_1 &= x_1 + x_2 + \cdots + x_n = \sigma_1, \\
\Sigma x_1x_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = \sigma_2, \\
\Sigma x_1x_2x_3 &= \sigma_3, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
x_1x_2x_3 \cdots x_n &= \sigma_n
\end{aligned}$$

are called the *elementary symmetric functions.*

We may define the *weight* of a power such as x_i^e to be $e(n + 1 - i)$ and the weight of a term to be the sum of the weights of the factors. Thus the weight of the term $x_1^3x_2^2x_3$ is $3(4 - 1) + 2(4 - 2) + 1(4 - 3) = 14$. Only a constant has weight 0. The weight of the product of two terms is clearly the sum of the weights of the factors.

Every sigma function contains one term of the form

$$x_1^{e_1}x_2^{e_2} \cdots x_i^{e_i}$$

where $e_1 \geqq e_2 \geqq \cdots \geqq e_i$. To see this, we select any term of the sigma function and arrange the factors so that it reads

$$x_{k_1}^{e_1}x_{k_2}^{e_2} \cdots x_{k_i}^{e_i},$$

where $e_1 \geqq e_2 \geqq \cdots \geqq e_i$. Since the sigma function contains all terms obtainable from this one by permutations of the subscripts, it contains

$$x_1^{e_1}x_2^{e_2} \cdots x_i^{e_i}.$$

The term just described, in which the indeterminates are in the order $x_1, x_2, \cdots, x_i$ and the exponents are non-increasing, is the unique term of highest weight in the sigma function, because every permutation that does not leave it unchanged will lower its weight.

We are now in a position to prove

Theorem 46. The Fundamental Theorem on Symmetric Functions. Every polynomial in the indeterminates $x_1, x_2, \cdots, x_n$ that has coefficients in a field F and is symmetric can be written as a polynomial in the elementary symmetric functions $\sigma_1, \sigma_2, \cdots, \sigma_n$ with coefficients in F.

Let f be a symmetric polynomial in $x_1, x_2, \cdots, x_n$, and let t_1 be one of its terms. Then f contains every term of Σt_1. If there is a term t_2 not in Σt_1, then f contains all the terms of Σt_2, none of which can be in Σt_1. Thus in a finite number of steps we obtain f written as a sum of sigma functions. Hence our theorem will be established when it is proved for a sigma function.

Let us assume that we have a sigma function whose unique term of highest weight is $x_1^3x_2^2x_3$, the exponents being non-increasing. The product

$$\sigma_3\sigma_2\sigma_1 = \Sigma x_1x_2x_3 \cdot \Sigma x_1x_2 \cdot \Sigma x_1$$

is a symmetric function whose unique term of highest weight is $x_1^3x_2^2x_3$. Then

$$\Sigma x_1^3x_2^2x_3 - \sigma_3\sigma_2\sigma_1 = -3x_1^2x_2^2x_3^2$$

is a symmetric function the weight of whose term of highest weight is lower than the weight of $x_1^3x_2^2x_3$. This symmetric function may be

written as a sum of sigma functions no one of which has a term of weight as high as that of $x_1^3x_2^2x_3$. We continue the process:

$$-3x_1^2x_2^2x_3^2 = -3\sigma_3^2.$$

Eventually we reach a symmetric function whose weight is 0, and which is therefore a constant. Upon transposing we have the result stated in the theorem:

$$\Sigma x_1^3x_2^2x_3 = \sigma_1\sigma_2\sigma_3 - 3\sigma^2.$$

The method is general.

40. Relations among the Roots

Let

$$f(x) = x^n + c_1x^{n-1} + c_2x^{n-2} + \cdots + c_{n-1}x + c_n$$

be a polynomial of degree n with complex coefficients. According to the fundamental theorem of algebra, $f(x)$ has a factor $x - r_1$ where r_1 is a complex number. Then

$$f(x) = g(x) \cdot (x - r_1)$$

where $g(x)$ is of degree $n - 1$. By the same argument, $g(x)$ has a factor $x - r_2$. After a repetition of the argument we see that there exist n complex numbers $r_1, r_2, \cdots, r_n$ such that

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_n).$$

By the unique factorization theorem for polynomials (Theorem 19) the r's are uniquely defined. These numbers are the *zeros* of the polynomial $f(x)$, and the *roots* of the equation $f(x) = 0$.

Let us now reverse the steps and multiply together the differences

$$(x - r_1)(x - r_2) \cdots (x - r_n).$$

There will be 2^n terms in the product, each term obtained by taking from each parenthesis either x or $-r_i$ and multiplying these together.

Thus in the product $(x - r_1)(x - r_2)$ there are $2^2 = 4$ terms,

$$f(x) = x^2 - r_1x - r_2x + r_1r_2 = x^2 - (r_1 + r_2)x + r_1r_2.$$

If we write $f(x) = x^2 + c_1x + c_2$, it is clear that

$$r_1 + r_2 = -c_1, \qquad r_1r_2 = c_2.$$

In the case of the cubic polynomial

$$f(x) = x^3 + c_1x^2 + c_2x + c_3 = (x - r_1)(x - r_2)(x - r_3),$$

we obtain eight terms upon multiplying out the linear factors, namely

$$x^3 - r_1x^2 - r_2x^2 - r_3x^2 + r_1r_2x + r_1r_3x + r_2r_3x - r_1r_2r_3.$$

After comparing coefficients, it is evident that

$$r_1 + r_2 + r_3 = -c_1, \qquad r_1r_2 + r_2r_3 + r_3r_1 = c_2, \qquad r_1r_2r_3 = -c_3.$$

41. Symmetric Functions of the Roots

In order to consider polynomials of degree n, we shall find it convenient to use the notation of symmetric functions. Let us set

$$\Sigma r_1 = r_1 + r_2 + \cdots + r_n = \sigma_1,$$

$$\Sigma r_1r_2 = r_1r_2 + r_1r_3 + \cdots + r_1r_n + r_2r_3 + \cdots + r_{n-1}r_n = \sigma_2,$$

$$\Sigma r_1r_2r_3 = r_1r_2r_3 + r_1r_2r_4 + \cdots = \sigma_3,$$

. . . . . .

where $\Sigma r_1r_2 \cdots r_i = \sigma_i$ denotes the sum of all distinct combinations of the letters $r_1, r_2, \cdots, r_n$ taken i at a time. Since there are

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}$$

combinations of n things taken i at a time, there are that many terms in each such sum. These sums we have called the elementary symmetric functions of the letters $r_1, r_2, \cdots, r_n$.

The product

$$(x - r_1)(x - r_2) \cdots (x - r_n)$$

contains 2^n terms. The terms which contain x^{n-i} will contain i products of distinct r's, and there will be a term for every combination of the r's. Hence the total coefficient of x^{n-i} will be

$$\pm\Sigma r_1r_2 \cdots r_i.$$

Since each r is taken with the minus sign, this coefficient will be

$$(-1)^i\Sigma r_1r_2 \cdots r_i.$$

Hence, if we write

$$f(x) = x^n + c_1x^{n-1} + \cdots + c_ix^{n-i} + \cdots + c_{n-1}x + c_n,$$

it will be true that $c_i = (-1)^i\sigma_i$. We have thus proved

Theorem 47. Every coefficient of $f(x)$ is equal to $\pm$ an elementary symmetric function of the roots of $f(x) = 0$.

At this point we may obtain as a by-product a very easy proof of the binomial theorem. If the roots of $f(x)$ are all equal to $-r$,

$$c_i = \binom{n}{i} r^i,$$

$$\begin{aligned} f(x) &= (x + r)^n \\ &= x^n + nrx^{n-1} + \frac{n(n-1)}{2} r^2 x^{n-2} + \frac{n(n-1)(n-2)}{6} r^3 x^{n-3} + \cdots \\ &= \sum_{i=0}^{n} \binom{n}{i} r^i x^{n-i}. \end{aligned}$$

Exercise 27

1. Form a cubic equation with the roots 2, -5, and 7.
2. Form a quartic equation with the roots $2 + 5i$, $2 - 5i$, 7, and -1.
3. The equation

$$x^3 - 2x^2 - 15x + 36 = 0$$

has a double root. Find it by using the relations among the roots.

4. Show that one root of $x^3 + bx^2 + cx + d = 0$ is the negative of another if and only if $d = bc$.

5. The difference of two roots of the equation $x^3 - 28x + 48 = 0$ is 2. Find the roots.

6. Find a quadratic equation whose roots are the squares of the roots of $x^2 + bx + c = 0$.

7. A teacher gave a quadratic equation to his class to solve. Student A copied down the coefficient of x incorrectly and obtained the roots 2 and 6. Student B copied down the constant term incorrectly and obtained the roots 2 and 5. What were the correct roots?

8. Take $x = r = 1$ in the binomial theorem and prove that

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n.$$

9. For $n = 4$ write out $\Sigma x_1 x_2 x_3$ and $\Sigma x_1^3 x_2 x_3^2$.

42. Newton's Formulas.

Next to the elementary symmetric functions, the most important symmetric functions are the sums of powers:

$$\begin{aligned} s_1 &= r_1 + r_2 + \cdots + r_n, \\ s_2 &= r_1^2 + r_2^2 + \cdots + r_n^2, \\ &\cdots\cdots\cdots\cdots \\ s_k &= r_1^k + r_2^k + \cdots + r_n^k. \end{aligned}$$

To this we shall add

$$s_0 = 1 + 1 + \cdots + 1 = n.$$

We shall derive a very ingenious set of recursive relations, due to Newton, by which these power sums may be calculated.

Lemma 1. If $r_1, r_2, \cdots, r_n$ are the roots of $f(x) = 0$, then

$$f'(x) = \sum_{i=1}^{n} \frac{f(x)}{x - r_i}.$$

If $f(x) = (x - r_1)(x - r_2) \cdots (x - r_n)$, then by the rules of the differential calculus
$f'(x) = (x - r_2) \cdots (x - r_n) + (x - r_1)(x - r_3) \cdots (x - r_n) + \cdots$, each term omitting just one factor $x - r_i$.

Lemma 2. If r is a root of $f(x) = x^n + c_1x^{n-1} + \cdots + c_n = 0$, then

$$\frac{f(x)}{x - r} = x^{n-1} + (r + c_1)x^{n-2} + (r^2 + c_1r + c_2)x^{n-3} + \cdots + (r^{n-1} + c_1r^{n-2} + \cdots + c_{n-1}).$$

This is immediate if we use synthetic division. Thus

$$\begin{array}{cccccc|c} 1 & c_1 & c_2 & c_3 & \cdots & & \\ & r & r^2 + c_1r & r^3 + c_1r^2 + c_2r & \cdots & & r \\ \hline 1 & r + c_1 & r^2 + c_1r + c_2 & r^3 + c_1r^2 + c_2r + c_3 & \cdots & & \end{array}$$

Since r is a root, the last term is $f(r) = 0$.

Lemma 3. The derivative of $f(x)$ is

$$f'(x) = nx^{n-1} + (s_1 + nc_1)x^{n-2} + (s_2 + c_1s_1 + nc_2)x^{n-3} + \cdots + (s_{n-1} + c_1s_{n-2} + \cdots + nc_{n-1}).$$

Replace r in Lemma 2 by r_i and sum for $i = 1, 2, \cdots, n$. By Lemma 1 the result is $f'(x)$.

Theorem 48. Newton's Identities.

$$s_k + c_1s_{k-1} + c_2s_{k-2} + \cdots + c_{k-1}s_1 + kc_k = 0 \qquad k > 0,$$

where c_j is to be replaced by 0 for all $j > n$.

Case I, $k = 1, 2, \cdots, n$. Clearly

$$f'(x) = nx^{n-1} + c_1(n - 1)x^{n-2} + c_2(n - 2)x^{n-3} + \cdots + c_{n-1}.$$

Upon comparing the coefficient of x^{n-k-1} above with the corresponding coefficient in $f'(x)$ as given in Lemma 3, we have

$$c_k(n-k) = s_k + c_1 s_{k-1} + \cdots + c_{k-1}s_1 + nc_k,$$

whence the theorem follows.

Case II, $k > n$. Since r_i is a root of $f(x) = 0$,

$$r_i^n + c_1 r_i^{n-1} + c^2 r^{n-2} + \cdots + c_n = 0.$$

Multiply through by r_i^{k-n}:

$$r_i^k + c_1 r_i^{k-1} + c_2 r^{k-2} + \cdots + c_n r_i^{k-n} = 0.$$

On summing for $i = 1, 2, \cdots, n$, we have

$$s_k + c_1 s_{k-1} + c_2 s_{k-2} + \cdots + c_n s_{k-n} = 0.$$

Exercise 28

1. Find the sum of the squares, the sum of the cubes, and the sum of the fourth powers of the roots of $x^3 - 2x^2 + 5x - 3 = 0$.

2. Let s_1, s_2, and s_3 be power sums of the roots of

$$x^3 + bx^2 + cx + d = 0.$$

Find b, c, and d in terms of s_1, s_2, and s_3.

3. The sum of three numbers is 6, the sum of their squares is 38 and the sum of their cubes is 144. Find the numbers. [Find an equation whose roots are the required numbers.]

4. If r_1, r_2, and r_3 are the roots of $x^3 + c_1x^2 + c_2x + c_3 = 0$, show that

$$\Sigma r_1^3 r_2^3 = c_2^3 - 3\Sigma r_1^3 r_2^2 r_3 - 6r_1^2 r_2^2 r_3^2 = c_2^3 - 3c_1c_2c_3 + 3c_3^2.$$

5. Show that

$$\Sigma r_1^4 r_2 r_3 = c_1^3 c_3 - 3\Sigma r_1^3 r_2^2 r_3 - 6r_1^2 r_2^2 r_3^2 = c_1^3 c_3 - 3c_1c_2c_3 + 3c_3^2.$$

6. Show that

$$\begin{aligned}\Sigma r_1^4 r_2^2 &= c_1^2 c_2^2 - 2\Sigma r_1^4 r_2 r_3 - 2\Sigma r_1^3 r_2^3 - 8\Sigma r_1^3 r_2^2 r_3 - 15 r_1^2 r_2^2 r_3^2 \\ &= c_1^2 c_2^2 - 2c_1^3 c_3 + 4c_1c_2c_3 - 3c_3^2 - 2c_2^3.\end{aligned}$$

7. Show that

$$\begin{aligned}(r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2 &= \Sigma r_1^4 r_2^2 - 2\Sigma r_1^4 r_2 r_3 - 2\Sigma r_1^3 r_2^3 + 2\Sigma r_1^3 r_2^2 r_3 - 6 r_1^2 r_2^2 r_3^2 \\ &= 18c_1c_2c_3 - 4c_1^3 c_3 + c_1^2 c_2^2 - 4c_2^3 - 27c_3^2.\end{aligned}$$

43. The Discriminant

Let

$$f(x) = x^n + c_1x^{n-1} + c_2x^{n-2} + \cdots + c_n = 0$$

have the roots $r_1, r_2, \cdots, r_n$. The function

$$\begin{aligned}\Delta = (r_1 - r_2)^2(r_1 - r_3)^2 \cdots (r_1 - r_n)^2 \\ (r_2 - r_3)^2 \cdots (r_2 - r_n)^2 \\ \cdots\cdots\cdots\cdots \\ (r_{n-1} - r_n)^2\end{aligned}$$

is called the *discriminant* of $f(x) = 0$. It is clear that $\Delta = 0$ when and only when $f(x) = 0$ has a multiple root. Since each difference is squared, Δ is a symmetric function of the roots and hence can be written as a polynomial in the coefficients. As was shown in Problem 7, § 42, the discriminant of the cubic $x^3 + c_1x^2 + c_2x + c_3 = 0$ is

$$\Delta = 18c_1c_2c_3 - 4{c_1}^3c_3 + {c_1}^2{c_2}^2 - 4{c_2}^3 - 27{c_3}^2.$$

For the reduced cubic $x^3 + px + q = 0$, the discriminant is

$$\Delta = -4p^3 - 27q^2.$$

Compare with Problem 6, § 29.

Theorem 49. If $f(x) = 0$ becomes $g(y) = 0$ under the transformation $x = y + h$, then $f(x) = 0$ and $g(y) = 0$ have equal discriminants.

For, if $f(x) = 0$ has the roots $r_1, r_2, \cdots, r_n$ and $g(y) = 0$ has the roots $s_1, s_2, \cdots, s_n$, then, for every i, $r_i = s_i + h$ for some arrangement of the roots, and, for every i and j,

$$r_i - r_j = s_i - s_j.$$

Hence

$$\Pi(r_i - r_j)^2 = \Pi(s_i - s_j)^2.$$

Corollary 49. If the cubic equation

$$x^3 + c_1x^2 + c_2x + c_3 = 0$$

is reduced to the form

$$y^3 + py + q = 0$$

by the transformation $x = y - c_1/3$, then the two cubics have equal discriminants.

Theorem 50. Let Δ be the discriminant of the cubic

$$f(x) = x^3 + c_1x^2 + c_2x + c_3 = 0$$

with real coefficients. If $\Delta = 0$, $f(x) = 0$ has a multiple root, which is necessarily real. If $\Delta > 0$, $f(x) = 0$ has three distinct real roots. If $\Delta < 0$, $f(x) = 0$ has one real root and one pair of conjugate complex (non-real) roots.

It was proved in Problem 6, § 29, that the reduced cubic has three real roots if and only if $\Delta > 0$. From the definition

$$\Delta = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2,$$

it is clear that there is a multiple root if and only if $\Delta = 0$. The remaining case, $\Delta < 0$, must then occur if and only if the cubic has just one real root and a pair of conjugate non-real roots. If there is a multiple root it must be real, for a non-real root is accompanied by its own conjugate of the same multiplicity, and a cubic cannot have four roots.

Since the addition of a real number h to each of the roots does not change their character, the criterion holds for all cubics.

Exercise 29

1. What is the discriminant of $x^3 - 2x - 2 = 0$?

2. Find the discriminant of $x^3 - 2x^2 - 5x + 7 = 0$, first directly from the formula, and then after having reduced the cubic equation.

3. If every real root of an equation $f(x) = 0$ with real coefficients and the real part of every non-real root is negative, show that all the coefficients of $f(x)$ have the same sign.

4. Let a cubic have the roots a, $b + ic$, and $b - ic$ where a, b, and c are real. Show directly from the definition of discriminant that Δ is 0 or < 0 according as $c = 0$ or $c \neq 0$.

5. Show that the discriminant of $x^2 + bx + c = 0$ is $b^2 - 4c$.

44. Solution of the Cubic by Radicals

Consider the reduced cubic

$$y^3 + py + q = 0 \qquad \Delta = -4p^3 - 27q^2$$

with real coefficients. If we substitute $y = z - p/3z$, we obtain the equation of degree 6:

$$z^6 + qz^3 - p^3/27 = 0.$$

This is a quadratic in z^3 so that we may write

$$z^3 = \tfrac{1}{2}(-q \pm \sqrt{q^2 + 4p^3/27}\,)$$
$$= -q/2 \pm \sqrt{-3\Delta}/18.$$

If $\Delta \leqq 0$, let z_1 be the real cube root of $-q/2 + \sqrt{-3\Delta}/18$, and let z_2 be the real cube root of $-q/2 - \sqrt{-3\Delta}/18$. If $\Delta > 0$, let z_1 be any cube root of $-q/2 + \sqrt{-3\Delta}/18$, and let z_2 be its conjugate, which is clearly a cube root of $-q/2 - \sqrt{-3\Delta}/18$. If we let $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$, then

$$z_1, z_2, z_3 = \omega z_1, \qquad z_4 = \omega z_2, \qquad z_5 = \omega^2 z_1, \qquad z_6 = \omega^2 z_2$$

all satisfy the sixth-degree equation for z and hence are its six complex roots.

The corresponding roots of the given cubic, namely

$$y_i = z_i - p/3z_i \qquad\qquad i = 1, 2, \cdots, 6$$

cannot be distinct, and it is not surprising that the six values of z fall into three sets of two values each, both z's of a set yielding the same value of y. It is easily calculated that

$$z_1 z_2 = z_3 z_6 = z_4 z_5 = -p/3$$

so that

$$y_1 = z_1 - p/3z_1 = z_1 - pz_2/3z_1z_2 = z_1 + z_2 = y_2,$$

and similarly

$$y_3 = \omega z_1 + \omega^2 z_2 = y_6, \qquad y_5 = \omega^2 z_1 + \omega z_2 = y_4.$$

If $\Delta < 0$, z_1 and z_2 are real and the given equation has one real root y_1 and two complex roots y_3 and y_5. If $\Delta > 0$, let $z_1 = a + bi$. Then $z_2 = a - bi$. The three real roots are then $y_1 = 2a$, $y_3 = -a - b\sqrt{3}$ and $y_5 = -a + b\sqrt{3}$ where a and b are real numbers but not usually expressible in terms of radicals with real radicands. If $\Delta = 0$, z_1 is the real cube root $\sqrt[3]{-q/2}$. Then $z_2 = z_1$ and the roots of the cubic are $y_1 = 2z_1$, $y_2 = z_1(\omega + \omega^2)$ and $y_5 = z_1(\omega^2 + \omega) = y_3$. Since $\omega^2 = \bar{\omega}$ and $\omega + \bar{\omega}$ is real, we see that the double root and the simple root are real.

These formulas, due to Tartaglia (1500–57), are fairly effective in solving a cubic whose discriminant is negative and which therefore has two non-real roots. It is not convenient in the case of a cubic with three real roots, for they are given as sums of non-real numbers. In fact, it is not possible to express exactly in terms of real radicals the roots of every rational cubic all of whose roots are real. Thus this method and the trigonometric method (§ 36) supplement each other.

Cubics with complex coefficients can be solved by this method but y should be calculated from the relation $y = z - p/3z$.

Example. Solve $x^3 - 7x - 7 = 0$.

We find $\Delta = 49$ so that all three roots are real.

$$z_1{}^3 = \tfrac{7}{2} + \tfrac{7}{18}\sqrt{-3} = 3.5 + 0.67358i.$$

Hence

$$x_1 = \sqrt[3]{3.5 + 0.67358i} + \sqrt[3]{3.5 - 0.67358i},$$

$$x_2 = \omega\sqrt[3]{3.5 + 0.67358i} + \omega^2\sqrt[3]{3.5 - 0.67358i},$$

$$x_3 = \omega^2\sqrt[3]{3.5 + 0.67358i} + \omega\sqrt[3]{3.5 - 0.67358i}$$

where $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$. Clearly the substitution of $-i$ for i in each of the three values for x merely permutes the terms, so that each x is real. The cube roots may be calculated trigonometrically and each value of x found in the form $a + bi$.

Exercise 30

1. Find in terms of radicals the roots of $x^3 - 12x - 34 = 0$.
2. Find in terms of radicals the roots of $x^3 - 6x + 2 = 0$.

Find the roots of each of the following equations in the form $a + bi$ where a and b are four-place decimals:

3. $x^3 + 3x - 2 = 0$.
4. $x^3 - x^2 - 4x + 1 = 0$.
5. $x^3 + 0.2138x + 0.6142 = 0$.
6. $x^3 + (71.31 + 28.39i)x - 131.4 + 719.68i = 0$.

45. The Quartic Equation

In § 37 we gave a method by which a reduced quartic function with real coefficients can be resolved into two real quadratic factors. Since the cubic can be solved by radicals, the values of k can be found in terms of radicals, and hence the zeros of the quadratic factors of the given quartic can be expressed in terms of radicals. This is interesting because the quartic is the equation of highest degree which in all cases can be solved in terms of radicals.

In resolving the quartic polynomial

$$x^4 + c_2x^2 + c_3x + c_4$$

into the quadratic factors

$$(x^2 + kx + p)(x^2 - kx + q),$$

we found that k^2 must be a root of the cubic equation

$$y^3 + 2c_2y^2 + (c_2^2 - 4c_4)y - c_3^2 = 0.$$

In fact, each of the six values for k leads to a factorization even though k, p, and q be complex. By the unique factorization theorem we know that these six values of k must correspond to the six possibilities for $x^2 - kx + q$, namely

$$(x - r_1)(x - r_2), \quad (x - r_1)(x - r_3), \quad (x - r_1)(x - r_4),$$
$$(x - r_2)(x - r_3), \quad (x - r_2)(x - r_4), \quad (x - r_3)(x - r_4).$$

Remembering that $r_1 + r_2 + r_3 + r_4 = 0$, we easily see that, if we let $k_1 = r_1 + r_2$, then $k_2 = -k_1 = r_3 + r_4$, so that the roots of the cubic are

$$y_1 = k_1^2 = (r_1 + r_2)^2 = (r_3 + r_4)^2,$$
$$y_2 = k_3^2 = (r_1 + r_3)^2 = (r_2 + r_4)^2,$$
$$y_3 = k_5^2 = (r_1 + r_4)^2 = (r_2 + r_3)^2.$$

Theorem 51. *The discriminant of the quartic equation*

$$x^4 + c_2x^2 + c_3x + c_4 = 0$$

is equal to the discriminant of the related cubic equation

$$y^3 + 2c_2y^2 + (c_2^2 - 4c_4)y - c_3^2 = 0.$$

We note that

$$\begin{aligned} y_1 - y_2 &= (r_1 + r_2)^2 - (r_1 + r_3)^2 \\ &= (r_1 + r_2 + r_1 + r_3)(r_1 + r_2 - r_1 - r_3) \\ &= (r_1 - r_4)(r_2 - r_3). \end{aligned}$$

Hence

$$(y_1 - y_2)^2(y_1 - y_3)^2(y_2 - y_3)^2 = \prod_{i<j}(r_i - r_j)^2.$$

But the latter is the discriminant of the quartic.

Exercise 31

1. Find the discriminant of the reduced quartic

$$x^4 - 3x^2 + x - 2 = 0.$$

2. Express the discriminant of $x^4 + c_2x^2 + c_3x + c_4 = 0$ as a polynomial in its coefficients.

3. Let $f(x) = 0$ with real coefficients have the distinct roots $a + ib$, $a - ib$, $c + id$, $c - id$. Show that the discriminant of $f(x) = 0$ is positive.

4. Let $f(x) = 0$ with real coefficients have two distinct real roots and two non-real roots. Show that the discriminant is negative.

5. Solve $x^4 - 25x^2 + 54x + 10 = 0$.

6. Solve $x^4 - 28x^2 + 36x + 7 = 0$.

7. Solve $x^4 + 3x^2 + 6x + 10 = 0$.

8. Solve $x^4 - 4.8672x^2 - 4.1735x + 28.8742 = 0$.

9. Solve $x^4 + (3.21 + 2.68i)x^2 + (5.66 - 4.34i)x - 10.38 + 12.57i = 0$.

CHAPTER

7

Systems of Higher Degree

46. Euclidean Rings

We have had two examples of what is called a *Euclidean ring.* The set of rational integers is such a ring. The set of all polynomials with coefficients in a field is also such a ring. In each instance the elements (numbers or polynomials as the case may be) are separated into four classes, zero, units, primes, and composites. In the ring of rational integers there are but two units, 1 and -1, while in the ring of polynomials there are infinitely many units, namely all numbers of the coefficient field except 0. In each case there exists an algorithm for the determination of the greatest common divisor, so that every pair of elements a and b have a g.c.d. expressible in the form

$$d = pa + qb$$

where p and q are in the ring. It follows in each case that, if a prime divides a product, it divides at least one of the factors. From this it follows that every composite element of the ring can be expressed as a product of prime (or irreducible) elements, and, except for unit factors and the order of the factors, this decomposition is unique.

A ring in which every composite element can be thus uniquely expressed as a product of primes is called a *unique factorization ring.* We shall see that there are unique factorization rings that are not Euclidean rings.

A unique factorization ring (and certain other rings also) can be extended to a field known as the *quotient field* of the ring. Thus the rational field is the quotient field of the ring of rational integers, and the set of all rational functions of x with coefficients in a field F is the quotient field of the ring of all polynomials in x with coefficients in F.

In Theorem 9 we showed essentially that, if the polynomial

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

with integral coefficients is divisible by the polynomial $qx - p$ where p and q are relatively prime integers, then the quotient is a polynomial whose first and last coefficients are integers. We can, in fact, prove much more than this. If a polynomial of degree n has coefficients in a unique factorization ring and is divisible by a polynomial of degree r whose coefficients are elements of the same ring and are relatively prime, then the quotient polynomial will also have all of its coefficients in the ring.

Theorem 52. If $f(x)\cdot g(x) = h(x)$ where $f(x)$, $g(x)$, and $h(x)$ have coefficients in a unique factorization ring, and if p is a prime which divides every coefficient of $h(x)$, then p divides every coefficient of $f(x)$ or every coefficient of $g(x)$.

Let

$$f(x) = a_0x^r + a_1x^{r-1} + \cdots + a_{r-1}x + a_r,$$
$$g(x) = b_0x^s + b_1x^{s-1} + \cdots + b_{s-1}x + b_s,$$
$$h(x) = c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n.$$

If $f(x)\cdot g(x) = h(x)$, then $n = r + s$ and

$$c_0 = a_0b_0, \qquad c_1 = a_0b_1 + a_1b_0, \qquad \cdots,$$
$$c_k = a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0$$

where we understand that $a_i = 0$ for $i > r$ and $b_j = 0$ for $j > s$.

Let us suppose that the prime number p divides every coefficient c_0, c_1, $\cdots$, c_n but that it does not divide every one of the numbers a_0, a_1, $\cdots$, a_r and also that it does not divide every one of the numbers b_0, b_1, $\cdots$, b_s. We prove the theorem by showing that this situation is impossible.

Suppose that p divides a_0, a_1, $\cdots$, a_{t-1} but does not divide a_t for some t, $0 \leqq t \leqq r$; and that p divides b_0, b_1, $\cdots$, b_{u-1} but does not divide b_u for some u, $0 \leqq u \leqq s$. Consider

$$c_{t+u} = a_0b_{t+u} + \cdots + a_tb_u + \cdots + a_{t+u}b_0.$$

Every term of this equation is 0 or is divisible by p except the term a_tb_u, which is not divisible by p since p does not divide either factor. Thus we have a contradiction.

Corollary 52. The Gauss Lemma. Let $f(x)\cdot g(x) = h(x)$ where $h(x)$ has coefficients in a unique factorization ring R, while $f(x)$ and $g(x)$ are assumed only to have coefficients in the quotient field of R. There exist polynomials, $f_1(x)$ of the same degree as $f(x)$, and $g_1(x)$ of the same degree

as $g(x)$, each with coefficients in R, such that

$$h(x) = f_1(x) \cdot g_1(x).$$

Let d be a least common denominator of the coefficients of $f(x)$, and let d_1 be a least common denominator of the coefficients of $g(x)$ so that

$$d \cdot f(x) = f_2(x), \qquad d_1 \cdot g(x) = g_2(x)$$

have coefficients in R, and

$$dd_1 \cdot h(x) = f_2(x) \cdot g_2(x).$$

Let p be a prime factor of dd_1. Then by the theorem p can be divided out either of all the coefficients of $f_2(x)$ or of all the coefficients of $g_2(x)$, and this can be continued until every prime factor of dd_1 has been divided out. Then

$$h(x) = f_1(x) \cdot g_1(x)$$

as stated.

47. Eisenstein's Criterion

It is not easy in general to determine when a polynomial is reducible and when it is irreducible. The following theorem is far from being a complete answer to this problem, but it is useful in some cases.

Theorem 53. Eisenstein. Suppose that

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

has coefficients in the unique factorization ring R. Suppose that there exists a prime p which divides every coefficient except a_0, and whose square does not divide a_n. Then $f(x)$ is irreducible in R.

If $f(x)$ is not factorable into two factors whose coefficients are in R, then it is irreducible in the quotient field of R by the Gauss lemma.

Let us suppose that

$$f(x) = a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$$

and that there is a prime p which divides a_1, a_2, a_3, a_4, and a_5 whose square does not divide a_5. Assume

$$f(x) = g(x) \cdot h(x)$$

where

$$g(x) = b_0x^3 + b_1x^2 + b_2x + b_3, \qquad h(x) = c_0x^2 + c_1x + c_2.$$

We shall show that p must also divide a_0, contradicting the hypothesis of the theorem.

We have

$$a_5 = b_3c_2, \qquad a_4 = b_2c_2 + b_3c_1, \qquad a_3 = b_1c_2 + b_2c_1,$$

$$a_2 = b_0c_2 + b_1c_1 + b_2c_0, \qquad a_1 = b_0c_1 + b_1c_0, \qquad a_0 = b_0c_0.$$

Since $p|a_5$ but p^2 does not divide a_5, p divides b_3 or c_2 but not both. Suppose that $p|b_3$ but not c_2. Since $p|a_4$, it follows that $p|b_2c_2$; but it is prime to c_2 so that $p|b_2$. Since $p|a_3$, $p|b_1$. Since $p|a_2$, $p|b_0$. Hence $p|a_0$, contrary to hypothesis.

The other alternative, namely that $p|c_2$ but not b_3, leads to the same conclusion.

The proof of the general theorem follows the same lines for a polynomial $f(x)$ of degree n and assumed factors $g(x)$ and $h(x)$, neither of which is of degree 0.

Corollary 53. For every positive integer n there are polynomials of degree n which are irreducible over the rational field.

Thus $x^n + 3x + 3$ is such an irreducible polynomial.

Evidently the situation in the rational field is different from that in the complex field or in the real field. In the complex field every polynomial of degree > 1 is reducible, and in the real field every polynomial of degree > 2 is reducible.

Exercise 32

1. $6x^2 + x - 15 = (\frac{6}{5}x + 2)(5x - \frac{15}{2})$. Write this polynomial as a product of two linear polynomials with integral coefficients.

2. Check for reducibility:

(a) $x^6 - 34x + 51$. (b) $x^3 - 375x^2 + 1250x + 80$.

(c) $y^3 + 2xy + x^2y + x + y + 1$.

3. Prove that $f(x)$ is reducible or irreducible according as $f(x - a)$ is reducible or irreducible. [In fact, if $f(x) = g(x) \cdot h(x)$, then $f(x - a) = g(x - a) \cdot h(x - a)$.]

4. Show that

$$x^3 - 6x^2 + 9x + 2$$

is irreducible by writing it in powers of $x - 1$.

5. Show that

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

is irreducible.

6. Show that

$$x^5 + x^4 + x^3 + x^2 + x + 1$$

is reducible.

7. Carry through the proof of Theorem 53 with $g(x)$ and $h(x)$ each of degree 3.

8. Show that in a unique factorization ring if $a|bc$ and $(a, b) = 1$, then $a|c$.

48. Content and Primitive Part

Let

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

be a polynomial whose coefficients belong to a unique factorization ring R. If a is a greatest common divisor of the coefficients $a_0, a_1, \cdots, a_n$, then a is called the *content* of the polynomial $f(x)$. It is unique up to a unit factor, and, if R is the ring of rational integers, the content may be taken as positive.

If the coefficients of $f(x)$ are relatively prime, i.e., if the content is a unit, then $f(x)$ is called a *primitive* polynomial. Every polynomial $f(x)$ may be written $a \cdot f_0(x)$ where a is the content of $f(x)$ and $f_0(x)$ is primitive. We shall call $f_0(x)$ the *primitive part* of $f(x)$. It is unique up to a unit factor. We shall hereafter use the subscript 0 to indicate that a polynomial is primitive. Clearly every divisor of a primitive polynomial is primitive.

Theorem 54. The product of two primitive polynomials is primitive.

Assume

$$f_0(x) \cdot g_0(x) = h(x)$$

where $f_0(x)$ and $g_0(x)$ are primitive. If $h(x)$ were not primitive, there would be a prime element p dividing each coefficient of $f_0(x)$ (which therefore could not be primitive) or dividing each coefficient of $g_0(x)$ by Theorem 52.

Theorem 55. If $f(x) \cdot g(x) = h(x)$, then the product of the contents of $f(x)$ and $g(x)$ is the content of $h(x)$, and the product of the primitive parts of $f(x)$ and $g(x)$ is the primitive part of $h(x)$.

Let

$$f(x) = a \cdot f_0(x), \qquad g(x) = b \cdot g_0(x), \qquad h(x) = c \cdot h_0(x)$$

where $f_0(x)$, $g_0(x)$ and $h_0(x)$ are primitive. Then

$$ab \cdot f_0(x) \cdot g_0(x) = c \cdot h_0(x).$$

Since $f_0(x)$ and $g_0(x)$ are primitive, their product is primitive by Theo-

rem 54. Since content and primitive part are unique up to unit factors,

$$ab = uc, \qquad f_0(x) \cdot g_0(x) = u^{-1} h_0(x)$$

where u is a unit. We may take ab to be the content of $h(x)$ and $h_0(x)$ to be its primitive part.

49. Greatest Common Divisor

We have defined the greatest common divisor $d(x)$ of two polynomials $f(x)$ and $g(x)$ by the properties

(i) $d(x) | f(x)$ and $d(x) | g(x)$,
(ii) if $e(x) | f(x)$ and $e(x) | g(x)$, then $e(x) | d(x)$.

Theorem 56. Let $f(x)$ and $g(x)$ be polynomials with coefficients in a unique factorization ring R. There exist polynomials $q(x)$ and $r(x)$ with coefficients in R where $r(x)$ is either 0 or of degree less than the degree of $g(x)$, and a number $k \neq 0$ of R, such that

$$k \cdot f(x) = g(x) \cdot q(x) + r(x).$$

By ordinary long division in the quotient field of R we determine polynomials $q_1(x)$ and $r_1(x)$ such that

$$f(x) = g(x) \cdot q_1(x) + r_1(x).$$

If k is a common denominator for the coefficients of $q_1(x)$ and $r_1(x)$, let $k \cdot q_1(x) = q(x)$ and $k \cdot r_1(x) = r(x)$ where $q(x)$ and $r(x)$ have coefficients in R, thus establishing the theorem. We may of course assume that k has no factor in common with the contents of both $q(x)$ and $r(x)$.

Theorem 57. Let $f_0(x)$ and $g_0(x)$ be two primitive polynomials, and let

$$k \cdot f_0(x) = g_0(x) \cdot q(x) + r(x).$$

If $f_0(x)$ and $g_0(x)$ have a g.c.d., it is a g.c.d. of $g_0(x)$ and the primitive part $r_0(x)$ of $r(x)$. Conversely a g.c.d. of $g_0(x)$ and $r_0(x)$ is a g.c.d. of $f_0(x)$ and $g_0(x)$.

Let $d_0(x)$ be a g.c.d. of $f_0(x)$ and $g_0(x)$. Then $d_0(x) | r(x)$ and hence divides its primitive part $r_0(x)$ by Theorem 55. Conversely let $d_{10}(x)$ be a g.c.d. of $g_0(x)$ and $r_0(x)$. Then $d_{10}(x) | k \cdot f_0(x)$, and hence $d_{10}(x) | f_0(x)$ by Theorem 55. Thus $d_0(x) | d_{10}(x)$ and $d_{10}(x) | d_0(x)$, so that $d_0(x)$ and $d_{10}(x)$ differ at most by a unit factor.

Corollary 57. Every two primitive polynomials have a g.c.d. This is primitive and unique up to a unit factor.

By Theorem 56 we obtain a finite chain of remainders

$$k_1 f_0(x) = g_0(x) \cdot q_1(x) + r(x),$$
$$k_2 g_0(x) = r_0(x) \cdot q_2(x) + r_1(x),$$
$$k_3 r_0(x) = r_{10}(x) \cdot q_3(x) + r_2(x),$$
$$\cdots\cdots\cdots\cdots\cdots$$

where each $r_i(x)$ is zero or of degree less than $r_{i-1}(x)$. In a finite number of steps a remainder of zero must be obtained. Then

$$(f_0(x), g_0(x)) = (g_0(x), r_0(x)) = (r_0(x), r_{10}(x)) = \cdots$$

so that the primitive part of the last non-zero remainder is equal to $(f_0(x), g_0(x))$.

Theorem 58. Let $f(x) = a \cdot f_0(x)$ and $g(x) = b \cdot g_0(x)$ where $f_0(x)$ and $g_0(x)$ are primitive. Let $d = (a, b)$ and $d_0(x) = (f_0(x), g_0(x))$. Then $d(x) = d \cdot d_0(x)$ is a g.c.d. of $f(x)$ and $g(x)$.

Clearly $d(x)$ is a common divisor of $f(x)$ and $g(x)$. Let $e(x) = e \cdot e_0(x)$ be any common divisor. Since $e_0(x) | f(x)$ and $g(x)$, then $e_0(x) | f_0(x)$ and $g_0(x)$ by Theorem 55, and hence $e_0(x) | d_0(x)$. Similarly $e | a$ and $e | b$, so that $e | d$. Hence $e(x) | d(x)$.

Corollary 58. Every two polynomials $f(x)$ and $g(x)$ not both 0 with coefficients in a unique factorization ring R have a g.c.d. which is unique up to a unit factor.

Example. Let

$$f(x) = 6x^4 + 12x^3 + 36x^2 + 48x + 48,$$
$$g(x) = 18x^3 + 9x^2 - 18x - 54.$$

Then

$$f(x) = 6(x^4 + 2x^3 + 6x^2 + 8x + 8) = 6 \cdot f_0(x),$$
$$g(x) = 9(2x^3 + x^2 - 2x - 6) = 9 \cdot g_0(x).$$

The content of the g.c.d. is $(6, 9) = 3$.

$$4f_0(x) = (2x + 3)g_0(x) + 25(x^2 + 2x + 2)$$

so that $r_0(x) = x^2 + 2x + 2$. Then

$$g_0(x) = (2x - 3)r_0(x).$$

Hence

$$(f(x), g(x)) = 3(x^2 + 2x + 2).$$

50. Unique Factorization

Theorem 59. Let $d(x)$ be a g.c.d. of $f(x)$ and $g(x)$. There exist polynomials $s(x)$ and $t(x)$ with coefficients in R, and a number $k \neq 0$ in R, such that

$$k \cdot d(x) = s(x) \cdot f(x) + t(x) \cdot g(x).$$

This follows in the usual way from the equations used in the proof of Corollary 57. Thus in the example of § 49,

$$25r_0(x) = 4f_0(x) - (2x + 3)g_0(x),$$

$$75d(x) = 2f(x) - (2x + 3)g(x).$$

Corollary 59. If $f(x)$ and $g(x)$ are relatively prime polynomials, there exist polynomials $s(x)$ and $t(x)$ also with coefficients in R, and a number $k \neq 0$ in R, such that

$$k = s(x) \cdot f(x) + t(x) \cdot g(x).$$

Theorem 60. If $f(x) | g(x) \cdot h(x)$ and if $f(x)$ and $g(x)$ are relatively prime, then $f(x) | h(x)$.

Since $f(x)$ and $g(x)$ are relatively prime, there is a number $k \neq 0$ such that

$$k = s(x) \cdot f(x) + t(x) \cdot g(x).$$

Hence

$$k \cdot h(x) = s(x) \cdot f(x) \cdot h(x) + t(x) \cdot g(x) \cdot h(x).$$

Thus $f(x)$ divides the right member and hence $f(x) | k \cdot h(x)$. Hence the primitive part $f_0(x)$ of $f(x)$ divides the primitive part $h_0(x)$ of $h(x)$. Moreover the content a of $f(x)$ divides the content of $g(x) \cdot h(x)$ and is relatively prime to the content of $g(x)$ so that it divides the content of $h(x)$. Thus $f(x) | h(x)$.

This is the key theorem in the proof of the uniqueness of factorization. By the same steps used in the proof of Theorem 7 or in the proof of Theorem 19, we may prove

Theorem 61. The ring of all polynomials with coefficients in a unique factorization ring is a unique factorization ring.

Corollary 61. Every polynomial $f(x, y, z, \cdots)$ in a finite number of indeterminates and with coefficients in a field or other unique factorization ring is uniquely factorable (save for units of the ring) into irreducible factors.

Exercise 33

1. Express the g.c.d. of $x^3 - 1$ and $3x - 3$ linearly in terms of the polynomials, i.e., in the form of Theorem 59.

2. Find a g.c.d. of the polynomials

$$3x^4 + 6x^3 - 3x, \qquad 2x^3 - 2x^2 - 2x + 2$$

with integral coefficients, and express it in the form of Theorem 59.

3. Do the same for

$$6x^4 + 9x^3 + 14x^2 + 11x - 15, \qquad 10x^3 + 21x^2 + 5x - 6.$$

4. Show that

$$x^3y^3 + 3x^2y^2 + x^2y - 6xy^2 - 5x - y^3 + 3y^2 - y + 5$$

considered as a polynomial in powers of x is primitive. Write it as a polynomial in powers of y, and find its content and its primitive part.

5. Show that

$$f(x, y) = 2x^2 + xy + y^2, \qquad g(x, y) = x^2 + y^2$$

are relatively prime, and find a polynomial $k(y) \neq 0$ and polynomials $s(x, y)$, $t(x, y)$ as in Corollary 59 such that

$$k(y) = s(x, y) \cdot f(x, y) + t(x, y) \cdot g(x, y).$$

6. Given

$$3x^3 + 2x^2y - xy^2 - 2xy + 6x^2, \qquad x^4 + x^3y + 2x^3 + x^2y^2 + xy^3 + 2xy^2$$

with rational coefficients. Considering them as polynomials in powers of x, find their g.c.d. and express it in the form of Theorem 59.

7. Consider the polynomials of Problem 6 as polynomials in powers of y, find their g.c.d., and express it in the form of Theorem 59.

8. Show that the ring of all polynomials in x with rational integral coefficients is a unique factorization ring which is not a Euclidean ring.

51. Systems of Equations

We shall now consider the solution of systems of equations of higher degree in two unknowns, such as

$$\begin{cases} x^3 + 3x^2 - y - 5 = 0, \\ x + 5x^2y + y^3 - 2 = 0. \end{cases}$$

The problem is considerably different from the problem of solving systems of linear equations.

Theorem 62. The system of polynomial equations

A: $$f(x, y) = 0, \qquad g(x, y) = 0$$

is equivalent to the system

$$B: \qquad f(x, y) = 0, \qquad s(x, y)\cdot f(x, y) + k\cdot g(x, y) = 0$$

where $s(x, y)$ is a polynomial and k is a field element not 0.

Clearly every solution (x_1, y_1) of system A is a solution of system B. A solution (x_2, y_2) of system B is a pair of numbers such that

$$f(x_2, y_2) = 0, \qquad s(x_2, y_2)\cdot f(x_2, y_2) + k\cdot g(x_2, y_2) = 0.$$

Then $k\cdot g(x_2, y_2) = 0$, and, if $k \neq 0$, $g(x_2, y_2) = 0$ so that (x_2, y_2) is a solution of system A.

Theorem 63. The system of equations

$$A: \qquad f(x, y) = 0, \qquad g(x, y)\cdot h(x, y) = 0$$

is equivalent to the two systems jointly:

$$B: \begin{cases} f(x, y) = 0, \\ g(x, y) = 0, \end{cases} \qquad C: \begin{cases} f(x, y) = 0, \\ h(x, y) = 0. \end{cases}$$

That is, every solution of A is a solution of B or of C, and every solution of B is a solution of A and every solution of C is a solution of A. The proof is evident.

Theorem 64. The system of equations

$$A: \qquad \begin{cases} f(x, y) = g(x, y), \\ f(x, y)\cdot p(x, y) = g(x, y)\cdot q(x, y) \end{cases}$$

is equivalent to the two systems jointly:

$$B: \begin{cases} f(x, y) = g(x, y), \\ p(x, y) = q(x, y), \end{cases} \qquad C: \begin{cases} f(x, y) = 0, \\ g(x, y) = 0. \end{cases}$$

For if we write system A in the form

$$\begin{cases} f(x, y)\cdot p(x, y) - g(x, y)\cdot q(x, y) = 0, \\ f(x, y) - g(x, y) = 0 \end{cases}$$

and subtract $q(x, y)$ times the second equation from the first, we have by Theorem 62 the equivalent system

$$\begin{cases} f(x, y)[p(x, y) - q(x, y)] = 0, \\ f(x, y) - g(x, y) = 0. \end{cases}$$

By Theorem 63 this is equivalent to B and C jointly.

Example. Solve the system of equations

$$\begin{cases} x^3 - y^3 = -3(x+1)y, \\ x^2 + xy + y^2 = x + 1. \end{cases}$$

By Theorem 64 this system is equivalent to the two systems jointly:

$$B: \begin{cases} x - y = -3y, \\ x^2 + xy + y^2 = x + 1, \end{cases} \qquad C: \begin{cases} x^2 + xy + y^2 = 0, \\ x + 1 = 0. \end{cases}$$

System B is equivalent to

$$\begin{cases} x = -2y, \\ 3y^2 + 2y - 1 = 0 \end{cases}$$

whose two solutions are $(2, -1)$ and $(-\frac{2}{3}, \frac{1}{3})$. System C is equivalent to

$$\begin{cases} x = -1, \\ y^2 - y + 1 = 0 \end{cases}$$

whose solutions are $(-1, \frac{1}{2} \pm \frac{1}{2}i\sqrt{3})$.

52. Systems of Symmetric Equations

If the unknowns occur symmetrically, the methods of solution just outlined may lead to equations of high degree, but the system is neatly solvable by the use of symmetric functions. The student should reread § 39 at this point.

Example 1. Solve

$$x + y = 5, \qquad xy = 6.$$

If we let $u^2 + c_1u + c_2 = 0$ be the quadratic equation whose roots are x and y, then clearly $c_1 = -(x + y) = -5$, $c_2 = 6$. The roots of

$$u^2 - 5u + 6 = 0$$

are $u_1 = 3$, $u_2 = 2$. Thus $(3, 2)$ is one of the solutions of the given system. Since the equations are symmetric, $(2, 3)$ is the other solution.

Example 2. Solve the system of symmetric equations

$$\begin{cases} x^2 + 3xy + y^2 + 2x + 2y = 8, \\ 2x^2 + 2y^2 + 3x + 3y = 14. \end{cases}$$

Since the left members are symmetric functions of x and y, they can be written as polynomials in the elementary symmetric functions:

$$c^2 + d - 2c = 8,$$

$$2c^2 - 4d - 3c = 14$$

where $x + y = -c$, $xy = d$. The solutions of this system are (c, d) $(-2, 0)$ and $(2\frac{3}{6}, 3\frac{5}{36})$. But x and y are the roots of the equation

$$u^2 + cu + d = 0.$$

From $u^2 - 2u = 0$ we obtain the two solutions $(x, y) = (0, 2)$ and $(2, 0)$, and from the equation $36u^2 + 138u + 35 = 0$ we obtain the solutions $(x, y) = (-0.273, -3.56)$ and $(-3.56, -0.273)$.

Exercise 34

Solve the following systems of equations:

1. $\begin{cases} x^2 + y^2 + x - 11y - 2 = 0, \\ x^2 - 5xy + 6y^2 = 0. \end{cases}$ [Factor the second equation.]

2. $\begin{cases} x^3 - y^3 = 63, \\ x - y = 3. \end{cases}$ [Use Theorem 64.]

3. $\begin{cases} x^2 + y^2 - 3 = 3xy, \\ 2x^2 - 6 + y^2 = 0. \end{cases}$ [Eliminate constant terms and factor.]

4. $\begin{cases} x^2 - 2y^2 = 4y, \\ 3x^2 + xy - 2y^2 = 16y. \end{cases}$ [Eliminate linear terms and factor.]

5. $\begin{cases} x^4 + x^2y^2 + y^4 = 7371, \\ x^2 - xy + y^2 = 63. \end{cases}$

6. $\begin{cases} x^2 - 3xy + y^2 = -1, \\ 3x^2 - xy + 3y^2 = 13. \end{cases}$

7. $\begin{cases} 21(x + y) = 10xy, \\ x + y + x^2 + y^2 = 68. \end{cases}$ [See § 52.]

8. $\begin{cases} xy + x + y + 19 = 0, \\ x^2y + xy^2 + 20 = 0. \end{cases}$

9. $\begin{cases} x + y + z = 3, \\ xy + yz + zx = -18, \\ x^2 + y^2 + z^2 = 45. \end{cases}$

10. $\begin{cases} x^2 + y^2 + z^2 = 69, \\ x^3 + y^3 + z^3 = -503, \\ x^4 + y^4 + z^4 = 4113. \end{cases}$ [See § 41.]

53. A General Method

We have discovered several methods for solving systems of equations of higher degree in two unknowns, but all of them were applicable only to equations of simple form. We shall now outline a method which is always applicable, although it may be more laborious than the special methods when the latter can be used.

Consider two polynomial equations

$$f(x, y) = 0, \qquad g(x, y) = 0.$$

If $f(x, y)$ and $g(x, y)$ have a greatest common divisor $d(x, y)$ so that

$$f(x, y) = d(x, y) \cdot f_1(x, y), \qquad g(x, y) = d(x, y) \cdot g_1(x, y),$$

it is clear that every solution of $d(x, y) = 0$ is a common solution of $f(x, y) = 0$ and $g(x, y) = 0$. If $d(x, y)$ is not a constant, the graphs of $f(x, y) = 0$ and $g(x, y) = 0$ will have a common arc.

Now let us suppose that $f(x, y)$ and $g(x, y)$ are relatively prime polynomials. The graphs of $f(x, y) = 0$ and $g(x, y) = 0$ will have no arc of finite length in common, but there may be points where the curves cross each other.

If we consider $f(x, y)$ and $g(x, y)$ to be polynomials in x whose coefficients are polynomials in y, we may by Theorem 59 determine polynomials $s(x, y)$, $t(x, y)$, and $k(y)$ such that

$$k(y) = s(x, y) \cdot f(x, y) + t(x, y) \cdot g(x, y).$$

Clearly if (x_1, y_1) is a solution of $f(x, y) = 0$ and $g(x, y) = 0$, then $k(y_1) = 0$. Since $k(y) = 0$ has but a finite number of solutions, the given system has but a finite number of solutions. In this way we determine where the curves cross each other.

By considering $f(x, y)$ and $g(x, y)$ to be polynomials in y whose coefficients are polynomials in x, we may determine polynomials $s_1(x, y)$, $t_1(x, y)$ and $k_1(x)$ such that

$$k_1(x) = s_1(x, y) \cdot f(x, y) + t_1(x, y) \cdot g(x, y).$$

Clearly the x co-ordinates of the crossing points satisfy the equation $k_1(x) = 0$. But not every solution of $k_1(x) = 0$ is to be paired with every solution of $k(y) = 0$. Ordinarily the easiest procedure is to determine one of these equations, say $k(y) = 0$, and then proceed to solve the system

$$f(x, y) = 0, \qquad g(x, y) = 0, \qquad k(y) = 0.$$

In many cases an even easier procedure is as follows:

Example 1. Find the common solutions of

$$\begin{cases} f(x, y) = y^3 - 3xy - 3y - x^3 = 0, \\ g(x, y) = y^2 + xy + x^2 - x - 1 = 0. \end{cases}$$

These functions are written as polynomials in y with coefficients that are polynomials in x. We proceed to find their g.c.d. considering y as the variable and x as a parameter. We find

$$f(x, y) = (y - x) \cdot g(x, y) - (x + 1)(2y + x).$$

Now, if $x = -1$, $g(x, y)$ is a divisor of $f(x, y)$ so that the solutions of

$$x = -1, \qquad g(-1, y) = y^2 - y + 1 = 0$$

are solutions of the given system. We thus obtain the solutions

$$(x, y) = (-1, \tfrac{1}{2}(1 + i\sqrt{3})), \qquad (-1, \tfrac{1}{2}(1 - i\sqrt{3})).$$

But, for values of $x \neq -1$, the g.c.d. of $f(x, y)$ and $g(x, y)$ is a g.c.d. of $g(x, y)$ and $2y + x$. We find that

$$4g(x, y) = (2y + x)^2 + (x - 2)(3x + 2).$$

Thus, if $x = 2$ or $x = -\frac{2}{3}$, $f(x, y)$ and $g(x, y)$ have the g.c.d. $2y + x$. From

$$x = 2, \qquad 2y + x = 0$$

we obtain the solution $(2, -1)$, and from

$$x = -\tfrac{2}{3}, \qquad 2y + x = 0$$

we obtain the solution $(-\frac{2}{3}, \frac{1}{3})$. There are no others. [See the example of § 51.]

On combining these steps we find that

$$(x - 2)(x + 1)(3x + 2) = (2y + x)f(x, y) + (x^2 + xy - 2y^2 + 4x + 4)g(x, y).$$

Thus

$$k_1(x) = (x - 2)(x + 2)(3x + 2).$$

Example 2. Find the singular points of the curve

$$x^3 + y^3 + 6x^2 + 3y^2 - 18xy + 21x - 6y = 0.$$

The singular points are the points common to $f(x, y) = 0$, $\partial f/\partial x = 0$, $\partial f/\partial y = 0$. That is, we are required to find the common solutions of

$$\begin{cases} f(x, y) = x^3 + y^3 + 6x^2 + 3y^2 - 18xy + 21x - 6y = 0, \\ g(x, y) = x^2 + 4x - 6y + 7 = 0, \\ h(x, y) = y^2 + 2y - 6x - 2 = 0. \end{cases}$$

Upon dividing we find that

$$f(x, y) - (y + 1)h(x, y) - (2x + 1)g(x, y) = -(x^3 + 3x^2 - 9x + 5),$$

$$h(x, y) + [\tfrac{1}{6}y + \tfrac{1}{36}(x^2 + 4x + 19)]g(x, y) = 36(x^4 + 8x^3 + 42x^2 - 112x + 61)$$

so that the given system is equivalent to

$$\begin{cases} x^3 + 3x^2 - 9x + 5 = 0, \\ x^4 + 8x^3 + 42x^2 - 112x + 61 = 0, \\ x^2 + 4x - 6y + 7 = 0. \end{cases}$$

The g.c.d. of the left members of the first two of these equations is $(x - 1)^2$ so that the system is equivalent to

$$\begin{cases} x = 1, \\ x^2 + 4x - 6y + 7 = 0. \end{cases}$$

Thus the only singular point on the cubic is (1, 2).

Exercise 35

1. Solve the system of equations

$$\begin{cases} x^2 + y = 8\frac{1}{3}, \\ x + y^2 = 34\frac{1}{36}. \end{cases}$$

2. Solve

$$a^2/x^2 + b^2/y^2 = 5, \qquad ab/xy = 2.$$

[The unknowns are a/x and b/y.]

3. Solve

$$2(x + y) = xy, \qquad x + y + x^2 + y^2 = 4.$$

4. Find the singular points of the curve

$$x^2 + 6x + y^2 + y^3 + 9 = 0.$$

5. Find the singular points of

$$x^4 + y^4 - 2x^2y + xy^2 + y^3 = 0.$$

6. The Hessian curve of $f(x, y) = 0$ intersects the latter in its singular points and inflection points. Find the singular points and inflection points of the curve

$$y^2 = x^3 - x^2$$

whose Hessian curve is

$$(3x - 1)y^2 = x^2.$$

7. Solve

$$\begin{cases} yx^3 - (y^3 - 3y - 1)x + y = 0, \\ x^2 - y^2 + 3 = 0. \end{cases}$$

8. Solve

$$\begin{cases} x^3 + 3yx^2 - 3x^2 + 3y^2x - 6xy - x + y^3 - 3y^2 - y + 3 = 0, \\ x^3 - 3yx^2 + 3x^2 + 3y^2x - 6xy - x - y^3 + 3y^2 + y - 3 = 0. \end{cases}$$

9. Find the intersection points of the confocal quadrics

$$\begin{cases} x^2/6 + y^2/3 + z^2 = 1, \\ x^2/4 + y^2 - z^2 = 1, \\ x^2/2 - y^2 - z^2/3 = 1. \end{cases}$$

54. The Resultant

Suppose that

$$f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m,$$
$$g(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n$$

are two polynomials with coefficients in a unique factorization domain. In some extended field F^* of this domain let $f(x)$ have the zeros α_1, α_2, $\cdots$, α_m, and let $g(x)$ have the zeros β_1, β_2, $\cdots$, β_n so that

$$g(x) = b_0(x - \beta_1)(x - \beta_2) \cdots (x - \beta_n).$$

The product

$$a_0{}^n b_0{}^m \Pi(\alpha_i - \beta_j) = a_0{}^n g(\alpha_1) \cdot g(\alpha_2) \cdots g(\alpha_m)$$

is called a *resultant* of $f(x)$ and $g(x)$, and is written

$$R(f(x), g(x)).$$

It is convenient to call any function which differs from this by a unit factor a resultant also. That is, the resultant has the same latitude of definition as the g.c.d.—it is unique up to a unit factor.

Theorem 65. The resultant $R(f(x), g(x))$ is a polynomial in the coefficients of $f(x)$ and $g(x)$.

Clearly

$$a_0{}^n g(\alpha_1) \cdot g(\alpha_2) \cdots g(\alpha_m)$$

is symmetric in the roots α_1, α_2, $\cdots$, α_m of $f(x) = 0$ and consequently can be written as a polynomial in the elementary symmetric functions

$$-a_1/a_0,\ a_2/a_0,\ -a_3/a_0,\ \cdots.$$

The maximal degree of each term in any one α_i is n so that the factor $a_0{}^n$ is sufficient to cancel all a_0's in the denominator, making $R(f(x), g(x))$ a polynomial in a_0, a_1, $\cdots$, a_m and b_0, b_1, $\cdots$, b_n.

Alternatively we may write

$$R(f(x), g(x)) = b_0{}^m f(\beta_1) \cdot f(\beta_2) \cdots f(\beta_n).$$

This function can differ from the one given above by a factor -1 at most.

Theorem 66. $R(f(x), g(x)) = 0$ *if and only if* $f(x) = 0$ *and* $g(x) = 0$ *have at least one root in common.*

This is evident from the form

$$R(f(x), g(x)) = a_0^n b_0^m \Pi(\alpha_i - \beta_j).$$

Since $a_0 \neq 0$ and $b_0 \neq 0$, R can be 0 if and only if some difference $\alpha_i - \beta_j$ is 0.

The function $k(y)$ of § 53 is closely related to the resultant. In that paragraph we had

$$k(y) = s(x, y) \cdot f(x, y) + t(x, y) \cdot g(x, y).$$

We considered these functions to be polynomials in x with coefficients which were polynomials in y. We may without loss of generality assume that no polynomial in y alone divides both $f(x, y)$ and $g(x, y)$, or both $s(x, y)$ and $t(x, y)$. For values of y for which $k(y) \neq 0$, $f(x, y)$ and $g(x, y)$ are relatively prime; while, for values of y for which $k(y) = 0$, $f(x, y)$ and $g(x, y)$ have a g.c.d. which is of degree at least 1 in x. Thus $k(y)$ vanishes when and only when $R(f(x, y), g(x, y))$ vanishes, and may be called an x *resultant* of $f(x, y)$ and $g(x, y)$.

Example. Find a resultant of

$$f(x) = a_0x^2 + a_1x + a_2, \qquad g(x) = b_0x^2 + b_1x + b_2.$$

By definition, if α_1 and α_2 are the roots of $f(x) = 0$,

$$\begin{aligned} R(f(x), g(x)) &= a_0^2(b_0\alpha_1^2 + b_1\alpha_1 + b_2)(b_0\alpha_2^2 + b_1\alpha_2 + b_2) \\ &= a_0^2[b_0^2\alpha_1^2\alpha_2^2 + b_0b_1\alpha_1\alpha_2(\alpha_1 + \alpha_2) \\ &\quad + b_0b_2(\alpha_1^2 + \alpha_2^2) + b_1^2\alpha_1\alpha_2 + b_1b_2(\alpha_1 + \alpha_2) + b_2^2]. \end{aligned}$$

Since

$$-a_0(\alpha_1 + \alpha_2) = a_1, \qquad a_0\alpha_1\alpha_2 = a_2,$$

we have

$$R = (a_0b_2 - a_2b_0)^2 - (a_0b_1 - a_1b_0)(a_1b_2 - a_2b_1).$$

By the method using the Euclid algorithm we have

$$b_0f(x) = a_0g(x) + (a_1b_0 - a_0b_1)x + a_2b_0 - a_0b_2,$$

$$\begin{aligned} (a_1b_0 - a_0b_1)^2g(x) &= [(a_1b_0 - a_0b_1)x + (a_2b_0 - a_0b_2)][(a_1b_0 - a_0b_1)b_0x \\ &\quad + b_1(a_1b_0 - a_0b_1) - b_0(a_2b_0 - a_0b_2)] \\ &\quad + b_0[(a_0b_2 - a_2b_0)^2 - (a_0b_1 - a_1b_0)(a_1b_2 - a_2b_1)]. \end{aligned}$$

Thus the remainder is the resultant R previously obtained multiplied by b_0.

55. The Discriminant

In several places we have encountered a function whose vanishing indicated that a certain polynomial $f(x)$ had a multiple zero. (§ 29, Problem 6, and § 43.) We defined the discriminant of a polynomial whose leading coefficient was 1 to be the product of the squares of the differences of the zeros, and showed that it could be expressed as a polynomial in the coefficients.

By Theorem 66 it is clear that the resultant of $f(x)$ and $f'(x)$ vanishes when and only when $f(x)$ has a multiple zero. Up to a non-vanishing factor, $R(f(x), f'(x))$ is the discriminant of $f(x)$.

The most satisfactory treatment of resultants and discriminants is by means of matrices and determinants, which are not treated in this book.

Exercise 36

1. Find the resultant of

$$a_0x^2 + a_1x + a_2, \qquad b_0x + b_1.$$

2. Use the answer to Problem 1 above to solve Problem 3, Exercise 35.

3. Solve Problem 6, Exercise 34, by means of the formula for the resultant of two quadratics developed in § 54.

4. Calculate the discriminant of

$$f(x) = x^3 + c_1x^2 + c_2x + c_3$$

by dividing $f(x)$ by $f'(x)$, etc.

5. Find the discriminant of

$$f(x) = x^3 + px + q$$

in the following manner: Let $f'(x)$ have the zeros α_1 and α_2, and use symmetric function theory to calculate $27f(\alpha_1) \cdot f(\alpha_2)$.

6. If $f(x) = q(x) \cdot g(x) + r(x)$, show that

$$R(f(x), g(x)) = R(r(x), g(x)).$$

7. Calculate the discriminant of the reduced quartic

$$f(x) = x^4 + c_2x^2 + c_3x + c_4.$$

Answers to Exercises

Exercise 1, p. 3.

2. $1 \pm \sqrt{17}$. **4.** $-\frac{5}{2} \pm \frac{1}{2}\sqrt{17}$. **6.** Every number. **8.** None. **9.** Every number except 5. **11.** None. **14.** 3.62, 512.55. **16c.** $x^2 - 2.9x - 31.08 = 0$.

Exercise 2, p. 8.

3. $(p, 2p)$. **4.** None. **6.** $I_1 = I_2 = 0.3324$.

Exercise 3, p. 13.

2. $(p, \frac{3}{4}p, \frac{1}{4}p)$. **3.** $(p, q, -2p + 3q)$. **6.** $(p, \frac{3}{2} - \frac{1}{2}p, q, 2 - q)$. **7.** $(p, \frac{11}{19} - \frac{11}{19}p, q, \frac{1}{19} - \frac{1}{19}p + \frac{1}{2}q)$. **10.** $x = 0.0424$, $y = -1.392$, $z = 0.449$.

Exercise 4, p. 15.

2. $(111411)_5$. **4.** $(463\alpha 7)_{12}$. **7.** $(11535623)_7$. **8.** $(0.53)_7$.

Exercise 5, p. 19.

1. $19 = 2 \cdot 437 - 9 \cdot 95$. **3.** $1 = -29 \cdot 91 + 44 \cdot 60$. (Answer is not unique.) **5.** $p_1 = 9$, $q_1 = 8$. **9.** $(25)_7$.

Exercise 6, p. 21.

1. $2 \cdot 5 \cdot 7^2 \cdot 11$. **2.** 48 in number. **7.** $x = 3$, $y = 2$, $z = 2$.

Exercise 7, p. 24.

1. 1, 2, −4. **2.** 4. **4.** 1, 2, 3, −3. **7.** None. **10.** $k = -289, -35, -23, -15, 13, 15, 17$.

Exercise 8, p. 25.

1. $0 < r < 3$. (There may be other correct answers to Problems 1, 3, and 5.) **3.** $-4 < r < 2.792$. **5.** $-9 < r < 5.8$. **7.** −4, −3, −2, 2, 7. **10.** 2.

Exercise 9, p. 28.

2. $\pm 1, \pm\frac{3}{2}$. **4.** $-1, \frac{2}{9}, 3, 4$. **6.** $(\frac{1}{2}, -\frac{1}{3})$. **8.** −6, 2, −4, 3.

Exercise 10, p. 34.

2. $q = x^3 + 2x^2 + 7$, $r = -1$. **4.** $q = x^4 + \frac{2}{25}$, $r = -\frac{1}{125}$. **10.** $(x^2 + x + 1)(x^2 - x + 3)$.

Exercise 11, p. 37.

1. $(x-2)^3+8(x-2)^2-3(x-2)-90$. **8.** $(x-2.1)^3-6.3(x-2.1)^2+11.23(x-2.1)+0.061$ **10.** $(x+1.11)^4-11.44(x+1.11)^3+36.7026(x+1.11)^2-37.664624(x+1.11)-0.28591259$. **12.** $(2x^2+x+1)(x^3+x+1)^2+(-5x^2+7)(x^3+x+1)+x^2-7x+1$.

Exercise 12, p. 40.

1. x^2-3x-1. **3.** x^3+x^2-x-1. **5.** $s=(-x+2)/4$, $t=\frac{1}{4}x$.

Exercise 13, p. 44.

1a. $2x-7+\dfrac{7x^2+2x+1}{x(x^2+x+1)}$. **1c.** Sum $=\dfrac{6x+1}{x^2+x+1}+\dfrac{1}{x}$.

3. $\dfrac{\frac{4}{9}x+\frac{2}{9}}{(x-1)^2}+\dfrac{-\frac{4}{9}}{x+2}$.

Exercise 14, p. 46.

2. $x=7/17$. **4.** 6, 40/13. **6.** None. **8.** 1, $-58/91$.

Exercise 15, p. 49.

1. $(x-1)(x+1)^2$. **3.** $(x+2)(x+1)=0$. **5.** $q=\pm 2$. **8.** 0, $-2a^7$.

Exercise 16, p. 52.

1. $2.64575\cdots$. **3.** $\frac{1}{3}(2+\sqrt{13})=1.86852\cdots$.

Exercise 17, p. 54.

3. max (0, 3), min (2, −1), inf (1, 1). **6.** No. Yes.

Exercise 18, p. 60.

1. 10, 3. **3.** 1. **7.** 1. **9.** 2. **12.** $x^3+9x^2+18x-9=0$.

Exercise 19, p. 64.

1. $f_1=3x^2-2$, $f_2=2x+3$, $f_3=-1$. **3.** (−3, −2), (1, 2), (2, 3).

Exercise 20, p. 66.

1. 1.7 and 1.8. **3.** −2.1 and −2, 1.1 and 1.2, 2.8 and 2.9. **5.** 1.9 and 2.

Exercise 21, p. 67.

1. 1.7693. **3.** 2.89195. **5.** 1.98734.

Exercise 22, p. 69.

1. 1.7693. **3.** 1.90782. **5.** 33.3579.

Exercise 23, p. 74.

1a. $3 - 2i$. **1b.** $2 + i\sqrt{5}$. **1c.** $1 - \frac{3}{2}i\sqrt{3}$. **4.** 1. **6a.** $4\pi/3$, 1. **6b.** $5\pi/3$ or 300°, 1.

Exercise 24, p. 78.

1. 1, $-\frac{1}{2} \pm i\frac{1}{2}\sqrt{3}$. **3.** -1.710, $0.853 \pm i1.477$. **5.** 2.768, -3.884, 1.116. **10.** 0.115, -3.861, -2.254. **11.** 1.9029.

Exercise 25, p. 80.

1. $(x^2 + \sqrt{2}x + 1 - \sqrt{2})(x^2 - \sqrt{2}x + 1 + \sqrt{2})$.
4. $(x^2 + 5.1255x + 8.5695)(x^2 - 1.1255x - 2.8005)$.
7. $[-2 - \sqrt{7} \pm i(\sqrt{2} + \sqrt{14})][-2 + \sqrt{7} \pm i(\sqrt{2} - \sqrt{14})]$.

Exercise 26, p. 82.

5. $2 - 3i$, $-3 - 2i$. **6.** $-0.8157 - 0.2906i$, $-0.5976 - 1.0519i$.

Exercise 27, p. 87.

2. $x^4 - 10x^3 + 46x^2 - 146x - 203 = 0$. **3.** 3, 3, -4. **5.** 2, 4, -6. **7.** 3, 4.

Exercise 28, p. 89.

2. $d = -\frac{1}{3}s_3 + \frac{1}{2}s_1s_2 - \frac{1}{6}s_1^3$. **3.** $x^3 - 6x^2 - x + 30 = 0$.

Exercise 29, p. 91.

1. -76. **2.** 761.

Exercise 30, p. 93.

1. $2\sqrt[3]{4} + \sqrt[3]{2}$, $2\omega\sqrt[3]{4} + \omega^2\sqrt[3]{2}$, $2\omega^2\sqrt[3]{4} + \omega\sqrt[3]{2}$. **3.** 0.5962, $-0.2981 \pm 1.8072i$.

Exercise 31, p. 94.

1. -8303. **7.** $-1 \pm i$, $1 \pm 2i$.

Exercise 32, p. 99.

1. $(3x + 5)(2x - 3)$.

Exercise 33, p. 104.

1. $3(x - 1) = 1 \cdot (3x - 1) + 0 \cdot (x^3 - 1)$. **2.** $6(x + 1) = (12x^2 + 21x + 3)g(x) - (8x - 10)f(x)$. **4.** Content is $x - 1$. **5.** $2y^4 = -(yx + y^2)f(x, y) + (3y^2 + 2yx)g(x, y)$.

Exercise 34, p. 107.

1. (3, 1), (−3/5, −1/5), (−2/5, −1/5), (4, 2). **3.** $(\sqrt{3}, 0)$, $(-\sqrt{3}, 0)$, $(\sqrt{3/19}, 6\sqrt{3/19})$, $(-\sqrt{3/19}, -6\sqrt{3/19})$. **6.** (−1, −2), (−2, −1), (1, 2), (2, 1). **8.** (5, −4), (−4, 5), $(-10 \pm 3\sqrt{11}, -10 \mp 3\sqrt{11})$. **9.** (0, 6, −3), (0, −3, 6), (6, 0, −3), (−3, 0, 6), (6, −3, 0), (−3, 6, 0).

Exercise 35, p. 110.

1. $(1, \frac{5}{3})$, $(2, -\frac{4}{3})$, $(-\frac{3}{2} \pm \frac{1}{6}\sqrt{21}, -\frac{1}{6} \pm \frac{1}{2}\sqrt{21})$. **3.** $(1, -2)$, $(-2, 1)$, $(2 \pm 2i, 2 \mp 2i)$. **4.** $(-3, 0)$. **6.** $(0, 0)$, $(\frac{4}{3}, \pm \frac{4}{9}\sqrt{3})$. **8.** $(0, \pm 1)$, $(0, 3)$, $(\pm 1, 0)$, $(\pm 2, 1)$, $(\pm 1, 2)$. **9.** Eight solutions, $(\pm\frac{4}{5}\sqrt{5}, \pm\frac{1}{2}\sqrt{2}, \pm\frac{1}{10}\sqrt{30})$.

Exercise 36, p. 113.

1. $a_0b_1^2 - a_1b_0b_1 + a_2b_0^2$. **7.** $16c_2^4c_4 + 256c_4^3 - 128c_2^2c_4^2 + 144c_2c_3^2c_4 - 4c_2^3c_3^2 - 27c_3^4$.

Index